

We only use cookies that are necessary for this site to function, and to provide you with the best experience. Learn more in our [Cookie Statement](#). By continuing to use this site, you consent to the use of cookies.



Subscribe to updates from
Cybersecurity and Infrastructure
Security Agency

Email Address e.g.
name@example.com

Subscribe

Vulnerability Summary for the Week of May 17, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 05/24/2021 12:55 PM EDT



You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of May 17, 2021

05/24/2021 07:05 AM EDT

Original release date: May 24, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cars-seller-auto-classifieds-script_project -- cars-seller-auto-classifieds-script	The request_list_request AJAX call of the Car Seller - Auto Classifieds Script WordPress plugin through 2.1.0, available to both authenticated and unauthenticated users, does not sanitise, validate or escape the order_id POST parameter before using it in a SQL statement, leading to a SQL Injection issue.	2021-05-14	7.5	CVE-2021-24285 MISC CONFIRM
kaswara_project -- kaswara	The Kaswara Modern VC Addons WordPress plugin through 3.0.1 allows unauthenticated arbitrary file upload via the 'uploadFontIcon' AJAX action. The supplied zipfile being unzipped in the wp-content/uploads/kaswara/fonts_icon directory with no checks for malicious files such as PHP.	2021-05-14	7.5	CVE-2021-24284 MISC CONFIRM
laobancms -- laobancms	Unrestricted File Upload in LAOBANCMS v2.0 allows remote attackers to upload arbitrary files by attaching a file with a ".jpg.php" extension to the component "admin/wenjian.php?wj=../templates/pc".	2021-05-14	7.5	CVE-2020-18166 MISC
linux -- linux_kernel	The block subsystem in the Linux kernel before 5.2 has a use-after-free that can lead to arbitrary code execution in the kernel context and privilege escalation, aka CID-c3e2219216c9. This is related to blk_mq_free_rqs and blk_cleanup_queue.	2021-05-14	7.2	CVE-2019-25044 MISC MISC MISC MISC
yfcmf -- yfcmf	YFCMF v2.3.1 has a Remote Command Execution (RCE) vulnerability in the index.php.	2021-05-14	7.5	CVE-2020-23691 MISC

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	The Photo Gallery by 10Web "Mobile-Friendly Image Gallery" WordPress plugin before 1.5.69 was vulnerable to Reflected Cross-Site Scripting (XSS) issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users)	2021-05-14	4.3	CVE-2021-24291 MISC CONFIRM
apache -- traffic_server	Apache Traffic Server 9.0.0 is vulnerable to a remote DOS attack on the experimental Slicer plugin.	2021-05-14	5	CVE-2021-27737 MISC MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dedecms -- dedecms	DedeCMS V5.7 SP2 contains a CSRF vulnerability that allows a remote attacker to send a malicious request to the web manager allowing remote code execution.	2021-05-15	6.8	CVE-2021-32073 MISC
express_handlebars_project -- express_handlebars	Express-handlebars is a Handlebars view engine for Express. Express-handlebars mixes pure template data with engine configuration options through the Express render API. More specifically, the layout parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only files with existing extensions (i.e. file.extension) can be included, files that lack an extension will have .handlebars appended to them. For complete details refer to the referenced GHSL-2021-018 report. Notes in documentation have been added to help users avoid this potential information exposure vulnerability.	2021-05-14	5	CVE-2021-32820 CONFIRM MISC MISC MISC MISC
express_handlebars_project -- express_handlebars	express-hbs is an Express handlebars template engine. express-hbs mixes pure template data with engine configuration options through the Express render API. More specifically, the layout parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only files with existing extensions (i.e. file.extension) can be included, files that lack an extension will have .hbs appended to them. For complete details refer to the referenced GHSL-2021-019 report. Notes in documentation have been added to help users of express-hbs avoid this potential information exposure vulnerability.	2021-05-14	4.3	CVE-2021-32817 MISC CONFIRM MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via bit_read_B ../../src/bits.c:135.	2021-05-17	6.8	CVE-2020-21841 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:48.	2021-05-17	6.8	CVE-2020-21818 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_revhistory ../../src/decode.c:3051.	2021-05-17	6.8	CVE-2020-21842 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via bit_calc_CRC ../../src/bits.c:2213.	2021-05-17	6.8	CVE-2020-21830 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2417.	2021-05-17	6.8	CVE-2020-21832 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via: read_2004_section_classes ../../src/decode.c:2440.	2021-05-17	6.8	CVE-2020-21833 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_preview ../../src/decode.c:3175.	2021-05-17	6.8	CVE-2020-21836 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via bit_search_sentinel ../../src/bits.c:1985.	2021-05-17	6.8	CVE-2020-21840 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via: read_2004_section_appinfo ../../src/decode.c:2842.	2021-05-17	6.8	CVE-2020-21838 MISC MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:51.	2021-05-17	6.8	CVE-2020-21819 MISC MISC
gnu -- libredwg	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:46.	2021-05-17	6.8	CVE-2020-21816 MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.10. Crafted input will lead to a memory leak in dwg_decode_eed ../../src/decode.c:3638.	2021-05-17	4.3	CVE-2020-21839 MISC MISC
gnu -- libredwg	A null pointer dereference issue exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2337.	2021-05-17	4.3	CVE-2020-21835 MISC MISC
gnu -- libredwg	A null pointer dereference issue exists in GNU LibreDWG 0.10 via get_bmp ../../programs/dwgbmp.c:164.	2021-05-17	4.3	CVE-2020-21834 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- libredwg	A null pointer dereference issue exists in GNU LibreDWG 0.10.2641 via <code>htmlscape ../../programs/escape.c:29</code> . which causes a denial of service (application crash).	2021-05-17	4.3	CVE-2020-21817 MISC MISC
gnu -- libredwg	A null pointer dereference issue exists in GNU LibreDWG 0.10.2641 via <code>output_TEXT ../../programs/dwg2SVG.c:114</code> , which causes a denial of service (application crash).	2021-05-17	4.3	CVE-2020-21815 MISC MISC
gnu -- libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via <code>bit_read_RC ../../src/bits.c:318</code> .	2021-05-17	6.8	CVE-2020-21843 MISC MISC
gnu -- libredwg	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via <code>htmlwescape ../../programs/escape.c:97</code> .	2021-05-17	6.8	CVE-2020-21814 MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of 'MatrixDiag*' operations(https://github.com/tensorflow/tensorflow/blob/4c4f420e68f1cfaf8f4b6e8e3eb857e9e4c3ff33/tensorflow/core/l197) does not validate that the tensor arguments are non-empty. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29515 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in 'tf.raw_ops.Conv2DBackpropInput'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/b40060c9f697b044e3107917c7976a054050295/tensorflow/l655) does a division by a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29525 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Missing validation between arguments to 'tf.raw_ops.Conv3DBackprop*' operations can result in heap buffer overflows. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/4814fab0ca6b5ab58a09411523b2103f2023f29520/tensorflow/l153) assumes that the 'input', 'filter_sizes' and 'out_backprop' tensors have the same shape, as they are accessed in parallel. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29520 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. In eager mode (default in TF 2.0 and later), session operations are invalid. However, users could still call the raw ops associated with them and trigger a null pointer dereference. The implementation(https://github.com/tensorflow/tensorflow/blob/eebb96c2830d48597d055d247c0e9aeb9ea94cd5/tensorflow/l203) fails to validate that indices used to access elements of input/output arrays are valid. Whereas accesses to 'input_backprop_flat' are guarded by 'FastBoundsCheck', the indexing in 'out_backprop_flat' can result in OOB access. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29516 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of 'tf.raw_ops.MaxPoolGrad' is vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/ab1e644b48c82cb71493f4362b4dd38f4577a1cf/tensorflow/l203) fails to validate that indices used to access elements of input/output arrays are valid. Whereas accesses to 'input_backprop_flat' are guarded by 'FastBoundsCheck', the indexing in 'out_backprop_flat' can result in OOB access. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29579 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor` (https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from outside the bounds of the `splits` tensor buffer in the implementation of the `RaggedBincount` (https://github.com/tensorflow/tensorflow/blob/8b677d79167799f712021d06a074476e0265413b16c/tensorflow/core/kernels/ragged_bincount_op.cc#L446). Before the `for` loop, `batch_idx` is set to 0. The attacker sets `splits(0)` to be 7, hence the `while` loop does not execute and `batch_idx` remains 0. This then results in writing to `out(-1, bin)`, which is before the heap allocated buffer for the output tensor. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.	2021-05-14	4.6	CVE-2021-29514 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedMul` by passing in invalid thresholds for the quantization. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/87cf4d3ea9949051e50ca3f071fc909538a51cd0/tensorflow/core/kernels/quantized_mul.cc#L290) assumes that the 4 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an empty buffer and accessing the element at position 0 results in overflow. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29535 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.AvgPool3DGrad` is vulnerable to a heap buffer overflow. The implementation (https://github.com/tensorflow/tensorflow/blob/d80ffba9702dc19d1fac74fc4b766b3fa1ee976b/tensorflow/core/kernels/avg_pool_grad.cc#L450) assumes that the `orig_input_shape` and `grad` tensors have similar first and last dimensions but does not check that this assumption is validated. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29577 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference by providing an invalid `permutation` to `tf.raw_ops.SparseMatrixSparseCholesky`. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/kernels/sparse_matrix_sparse_cholesky.cc#L86) fails to properly validate the input arguments. Although `ValidateInputs` is called and there are checks in the body of this function, the code proceeds to the next line in `ValidateInputs` since `OP_REQUIRES` (https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/kernels/sparse_matrix_sparse_cholesky.cc#L48) is a macro that only exits the current function. Thus, the first validation condition that fails in `ValidateInputs` will cause an early return from that function. However, the caller will continue execution from the next line. The fix is to either explicitly check `context->status()` or to convert `ValidateInputs` to return a `Status`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29530 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in `tf.raw_ops.QuantizedResizeBilinear` by manipulating input values so that float rounding results in off-by-one error in accessing image elements. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized_resize_bilinear.cc#L66) computes two integers (representing the upper and lower bounds for interpolation) by ceiling and flooring a floating point value. For some values of `in`, `interpolation->upper[i]` might be smaller than `interpolation->lower[i]`. This is an issue if `interpolation->upper[i]` is capped at `in_size-1` as it means that `interpolation->lower[i]` points outside of the image. Then, in the interpolation code (https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized_resize_bilinear.cc#L264), this would result in heap buffer overflow. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29529 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor` (https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from outside the bounds of the `splits` tensor buffer in the implementation of the `RaggedBincount` op (https://github.com/tensorflow/tensorflow/blob/8b677d79167799f712021d06074476e042654133/tensorflow/core/kernels/ragged_bincount_op.cc). Before the `for` loop, `batch_idx` is set to 0. The user controls the `splits` array, making it contain only one element, 0. Thus, the code in the `while` loop would increment `batch_idx` and then try to read `splits(1)`, which is outside of bounds. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.	2021-05-14	4.6	CVE-2021-29512 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedReshape` by passing in invalid thresholds for the quantization. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/a324ac84e573fba362a5e53d4e74d5de6729933e/tensorflow/core/kernels/quantized_reshape.cc) assumes that the 2 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an empty buffer and accessing the element at position 0 results in overflow. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29536 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPool3DGradGrad` is vulnerable to a heap buffer overflow. The implementation (https://github.com/tensorflow/tensorflow/blob/596c05a159b6fb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/max_pool_grad_grad.cc) does not check that the initialization of `Pool3dParameters` completes successfully. Since the constructor (https://github.com/tensorflow/tensorflow/blob/596c05a159b6fb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/max_pool_grad_grad.cc) uses `OP_REQUIRES` to validate conditions, the first assertion that fails interrupts the initialization of `params`, making it contain invalid data. In turn, this might cause a heap buffer overflow, depending on default initialized values. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29576 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedResizeBilinear` by passing in invalid thresholds for the quantization. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/50711818d2e61ccce012591eeb4095a2096724587/tensorflow/core/kernels/quantized_resize_bilinear.cc) assumes that the 2 arguments are always valid scalars and tries to access the numeric value directly. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29587 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow to occur in `Conv2DBackpropFilter`. This is because the implementation (https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv2d_backprop_filter.cc) computes the size of the filter tensor but does not validate that it matches the number of elements in `filter_sizes`. Later, when reading/writing to this buffer, code uses the value computed here, instead of the number of elements in the tensor. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29540 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger an integer division by zero undefined behavior in `tf.raw_ops.QuantizedBiasAdd`. This is because the implementation of the Eigen kernel(https://github.com/tensorflow/tensorflow/blob/61bca8bd5ba8a68b2d97435ddafcd2b8567266/tensorflow/core/kernels/eigen_bias.cc#L849) does a division by the number of elements of the smaller input (based on shape) without checking that this is not zero. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29546 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.SparseSplit`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/699bf5d961f0abfde8fa3f876e6d2c168/tensorflow/core/kernels/eigen_sparse_split.cc#L530) accesses an array element based on a user controlled offset. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29559 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can write outside the bounds of heap allocated arrays by passing invalid arguments to `tf.raw_ops.Dilation2DBackpropInput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/afd954e65f15aea4d438d0a219136fc4a63a573d/tensorflow/core/kernels/eigen_dilation2d_backprop.cc#L322) does not validate before writing to the output array. The values for `h_out` and `w_out` are guaranteed to be in range for `out_backprop` (as they are loop indices bounded by the size of the array). However, there are no similar guarantees relating `h_in_max`/`w_in_max` and `in_backprop`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29566 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger undefined behavior by binding to null pointer in `tf.raw_ops.ParameterizedTruncatedNormal`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/3f6fe4dfe6f657e768260b48166c27d148f3015f/tensorflow/core/kernels/eigen_parameterized_truncated_normal.cc#L130) does not validate input arguments before accessing the first element of `shape`. If `shape` argument is empty, then `shape_tensor.flat<T>()` is an empty array. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29568 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/31bd5026304677faa8a0b77602c6154171b9aec1/tensorflow/core/kernels/eigen_max_pool_grad.cc#L130) assumes that the last element of `boxes` input is 4, as required by [the op] (https://www.tensorflow.org/api_docs/python/tf/raw_ops/DrawBoundingBoxesV2). Since this is not checked attackers passing values less than 4 can write outside of bounds of heap allocated objects and cause memory corruption. If the last dimension in `boxes` is less than 4, accesses similar to `tboxes(b, bb, 3)` will access data outside of bounds. Further during code execution there are also writes to these indices. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29571 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPool3DGradGrad` exhibits undefined behavior by dereferencing null pointers backing attacker-supplied empty tensors. The implementation(https://github.com/tensorflow/tensorflow/blob/72fe792967e7fd2523434206880607b5802669574/tensorflow/core/kernels/eigen_max_pool_3d_grad_grad.cc#L703) fails to validate that the 3 tensor inputs are not empty. If any of them is empty, then accessing the elements in the tensor results in dereferencing a null pointer. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29574 MISC CONFIRM

<https://content.govdelivery.com/accounts/USDHSCISA/bulletins/2dc4ff3>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. TFLite's convolution code(https://github.com/tensorflow/tensorflow/blob/09c73bca7d648e961dd05898292d91a8322a9d45/tensorflow/lite/ke) has multiple division where the divisor is controlled by the user and not checked to be non-zero. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29594 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'BatchToSpaceNd' TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/b5ed552fe55895aee8bd8b191f744a069957d18d/tensorflow/lite/ker). An attacker can craft a model such that one dimension of the 'block' input is 0. Hence, the corresponding value in 'block_shape' is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29593 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The fix for CVE-2020-15209(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15209) missed the case when the target shape of 'Reshape' operator is given by the elements of a 1-D tensor. As such, the fix for the vulnerability(https://github.com/tensorflow/tensorflow/blob/9c1dc920d2ff24893dc9d27416039601526743/tensorflow/l) allowed passing a null-buffer-backed tensor with a 1D shape. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29592 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. TFLite graphs must not have loops between nodes. However, this condition was not checked and an attacker could craft models that would result in infinite loop during evaluation. In certain cases, the infinite loop would be replaced by stack overflow due to too many recursive calls. For example, the 'While' implementation(https://github.com/tensorflow/tensorflow/blob/106d8f4fb89335a2c52d7c895b7a7485465ca8d9/tensorfi) could be tricked into a scenario where both the body and the loop subgraphs are the same. Evaluating one of the subgraphs means calling the 'Eval' function for the other and this quickly exhaust all stack space. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range. Please consult our security guide(https://github.com/tensorflow/tensorflow/blob/master/SECURITY.md) for more information regarding the security model and how to contact us with issues and questions.	2021-05-14	4.6	CVE-2021-29591 CONFIRM MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Optimized pooling implementations in TFLite fail to check that the stride arguments are not 0 before calling 'ComputePaddingHeightWidth' (https://github.com/tensorflow/tensorflow/blob/3f24ccd932546416ec906a02ddd183b48). Since users can craft special models which will have 'params->stride_{height,width}' be zero, this will result in a division by zero. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29586 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The reference implementation of the 'GatherNd' TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/ker). An attacker can craft a model such that 'params' input would be an empty tensor. In turn, 'params_shape.Dims(.)' would be zero, in at least one dimension. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29585 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The optimized implementation of the 'TransposeConv' TFLite operator is [vulnerable to a division by zero error] (https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/L5222). An attacker can craft a model such that 'stride_{h,w}' values are 0. Code calling this function must validate these arguments. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29588 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The 'Prepare' step of the 'SpaceToDepth' TFLite operator does not check for 0 before division (https://github.com/tensorflow/tensorflow/blob/5f7975d09eac0f10ed8a17dbb6f59649777256d2021sa095a/L67). An attacker can craft a model such that 'params->block_size' would be zero. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29587 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'EmbeddingLookup' TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/e4b29809543b250bc9b19678ec4776299dd596a2021sa095a/L74). An attacker can craft a model such that the first dimension of the 'value' input is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29590 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in Eigen implementation of 'tf.raw_ops.BandedTriangularSolve'. The implementation (https://github.com/tensorflow/tensorflow/blob/ecb7ec454e6617738554a255d77f08e60ee0808/tensorflow/lite/kernels/BandedTriangularSolve.cc#L278) calls 'ValidateInputTensors' for input validation but fails to validate that the two tensors are not empty. Furthermore, since 'OP_REQUIRES' macro only stops execution of current function after setting 'ctx->status()' to a non-OK value, callers of helper functions that use 'OP_REQUIRES' must check value of 'ctx->status()' before continuing. This doesn't happen in this op's implementation (https://github.com/tensorflow/tensorflow/blob/ecb7ec454e6617738554a255d77f08e60ee0808/tensorflow/lite/kernels/BandedTriangularSolve.cc#L278). The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29612 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite computation for size of output after padding, 'ComputeOutSize' (https://github.com/tensorflow/tensorflow/blob/0c9692ae7b1671c983569e5d3de5565843d500cf/tensorflow/lite/kernels/ComputeOutSize.cc#L55), does not check that the 'stride' argument is not 0 before doing the division. Users can craft special models such that 'ComputeOutSize' is called with 'stride' set to 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29585 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'DepthToSpace' TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/L69). An attacker can craft a model such that 'params->block_size' is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29593 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB read on heap in the TFLite implementation of 'Split_V' (https://github.com/tensorflow/tensorflow/blob/c59c37e7b2d563967da813fa50fe20b21f4da683/tensorflow/lite/kernels/Split_V.cc#L150). If 'axis_value' is not a value between 0 and 'NumDimensions(input)', then the 'SizeOfDimension' function (https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39f4c3ab/tensorflow/lite/kernels/SizeOfDimension.cc#L150) will access data outside the bounds of the tensor shape array. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29606 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'SpaceToBatchNd' TFLite operator is [vulnerable to a division by zero error] (https://github.com/tensorflow/tensorflow/blob/412c7d9bb8f8a762c5b266c9e73bfa165f29aac8/tensorflow/lite/kernels/space_to_batch_nd.cc#L83). An attacker can craft a model such that one dimension of the 'block' input is 0. Hence, the corresponding value in 'block_shape' is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29597 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'SVDF' TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/7f283ff806b2031f407db64c4d3edcda8fb9f5/tensorflow/lite/kernels/svd.cc#L102). An attacker can craft a model such that 'params->rank' would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29598 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'Split' TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/e2752089ef7ce9bcb3db0ec618ebd23ea119cd/tensorflow/lite/kernels/split.cc#L65). An attacker can craft a model such that 'num_splits' would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29599 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the 'OneHot' TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/f61c57bd425878be108ec787f4d96390579fb83e/tensorflow/lite/kernels/one_hot.cc#L72). An attacker can craft a model such that at least one of the dimensions of 'indices' would be 0. In turn, the 'prefix_dim_size' value would become 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29600 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB write on heap in the TFLite implementation of 'ArgMin'/'ArgMax' (https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39cc65ab/tensorflow/lite/kernels/arg.cc#L59). If 'axis_value' is not a value between 0 and 'NumDimensions(input)', then the condition in the 'if' is never true, so code writes past the last valid element of 'output_dims->data'. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29603 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in 'SparseAdd' results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data. The implementation (https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/lite/kernels/sparse_add.cc#L102) has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of '*_indices' matches the size of corresponding '*_shape'. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29607 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.RaggedTensorToTensor`, an attacker can exploit an undefined behavior if input arguments are empty. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/ragged_to_tensor_op.cc#L360) only checks that one of the tensors is not empty, but does not check for the other ones. There are multiple `DCHECK` validations to prevent heap OOB, but these are no-op in release builds, hence they don't prevent anything. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick these commits on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29609 MISC MISC CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/sparse_add_op.cc#L100) has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29609 MISC CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalAvgPoolGrad` is vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/dcb796a28364d6d7f003f6fe733d3082f2008a729579/tensorflow/core/kernels/fractional_avg_pool_grad_op.cc#L100) fails to validate that the pooling sequence arguments have enough elements as required by the `out_backprop` tensor shape. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	4.6	CVE-2021-29609 MISC CONFIRM
hexagon -- intergraph_glnius	Hexagon Glnius Auskunftsportal before 5.0.0.0 allows SQL injection via the GiPWorkflow/Service/DownloadPublicFile id parameter.	2021-05-14	5	CVE-2021-32051 MISC MISC MISC
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 199235.	2021-05-14	4.3	CVE-2021-20564 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a privileged user to inject malicious data using a specially crafted HTTP request due to improper input validation.	2021-05-14	4	CVE-2020-4811 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 199236.	2021-05-14	5	CVE-2021-20565 XF CONFIRM
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 could allow an attacker to obtain sensitive information due to accepting body parameters in a query. IBM X-Force ID: 192642.	2021-05-14	5	CVE-2020-4985 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could disclose sensitive information due an overly permissive cross-domain policy. IBM X-Force ID: 196334.	2021-05-14	5	CVE-2021-20429 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196001.	2021-05-14	5	CVE-2021-20393 CONFIRM XF
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-05-14	4.3	CVE-2021-20392 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imagemagick -- imagemagick	In ImageMagick versions before 7.0.9-0, there are outside the range of representable values of type 'float' at MagickCore/quantize.c.	2021-05-14	4.3	CVE-2020-27769 MISC
kaspersky -- password_manager	Password generator feature in Kaspersky Password Manager was not completely cryptographically strong and potentially allowed an attacker to predict generated passwords in some cases. An attacker would need to know some additional information (for example, time of password generation).	2021-05-14	5	CVE-2020-27020 MISC
mikrotik -- routers	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-18	4	CVE-2020-20222 MISC MISC FULLDISC
mikrotik -- routers	Mikrotik RouterOs stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/diskd process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.	2021-05-18	4	CVE-2020-20227 MISC FULLDISC MISC
mikrotik -- routers	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20237 MISC MISC FULLDISC
mikrotik -- routers	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20236 MISC MISC FULLDISC
mikrotik -- routers	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the log process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20245 MISC FULLDISC MISC
mikrotik -- routers	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the mactel process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.	2021-05-18	4	CVE-2020-20246 MISC FULLDISC MISC
mikrotik -- routers	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from an assertion failure vulnerability in the btest process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	2021-05-18	4	CVE-2020-20214 MISC MISC FULLDISC
mikrotik -- routers	Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/bfd process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-18	4	CVE-2020-20220 MISC FULLDISC MISC
mooveagency -- redirect_404_to_parent	The settings page of the Redirect 404 to parent WordPress plugin before 1.3.1 did not properly sanitise the tab parameter before outputting it back, leading to a reflected Cross-Site Scripting issue	2021-05-14	4.3	CVE-2021-24286 CONFIRM
mooveagency -- select_all_categories_and_taxonomy	The settings page of the Select All Categories and Taxonomies, Change Checkbox to Radio Buttons WordPress plugin before 1.3.2 did not properly sanitise the tab parameter before outputting it back, leading to a reflected Cross-Site Scripting issue	2021-05-14	4.3	CVE-2021-24287 CONFIRM
moxa -- nport_ia5150a_firmware	By exploiting a vulnerability in NPort IA5150A/IA5250A Series before version 1.5, a user with "Read Only" privilege level can send requests via the web console to have the device's configuration changed.	2021-05-14	4	CVE-2020-27149 MISC MISC
moxa -- nport_ia5150a_firmware	Cleartext transmission of sensitive information via Moxa Service in NPort IA5000A series serial devices. Successfully exploiting the vulnerability could enable attackers to read authentication data, device configuration, and other sensitive data transmitted over Moxa Service.	2021-05-14	5	CVE-2020-27185 MISC MISC
quersol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the import_from_debug AJAX action to inject PHP objects.	2021-05-14	6.5	CVE-2021-24280 CONFIRM MISC
quersol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the various AJAX actions in the plugin to do a variety of things. For example, an attacker could use wpcf7r_reset_settings to reset the plugin's settings, wpcf7r_add_action to add actions to a form, and more.	2021-05-14	6.5	CVE-2021-24282 MISC CONFIRM
quersol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, unauthenticated users can use the wpcf7r_get_nonce AJAX action to retrieve a valid nonce for any WordPress action/function.	2021-05-14	5	CVE-2021-24278 MISC CONFIRM
quersol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, low level users, such as subscribers, could use the import_from_debug AJAX action to install any plugin from the WordPress repository.	2021-05-14	4	CVE-2021-24279 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
quersol -- redirection_for_contact_form_7	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the delete_action_post AJAX action to delete any post on a target site.	2021-05-14	4	CVE-2021-24281 MISC CONFIRM
squirrely -- squirrely	Squirrely is a template engine implemented in JavaScript that works out of the box with ExpressJS. Squirrely mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options remote code execution may be triggered in downstream applications. There is currently no fix for these issues as of the publication of this CVE. The latest version of squirrely is currently 8.0.8. For complete details refer to the referenced GHSL-2021-023.	2021-05-14	6.8	CVE-2021-32819 MISC MISC
tp-link -- archer_c1200_firmware	TP-Link Archer C1200 firmware version 1.13 Build 2018/01/24 rel.52299 EU has a XSS vulnerability allowing a remote attacker to execute arbitrary code.	2021-05-14	4.3	CVE-2020-17891 MISC
upx_project -- upx	A heap buffer overflow read was discovered in upx 4.0.0, because the check in p_lx_elf.cpp is not perfect.	2021-05-14	5.8	CVE-2020-24119 CONFIRM
wp-buy -- conditional_marketing_mailer	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WooCommerce Conditional Marketing Mailer WordPress plugin before 1.5.2, to install any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnerabilities like RCE.	2021-05-14	6.5	CVE-2021-24190 CONFIRM
wp-buy -- visitor_traffic_real_time_statistics	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Visitor Traffic Real Time Statistics WordPress plugin before 2.12, to install any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnerabilities like RCE.	2021-05-14	6.5	CVE-2021-24193 CONFIRM
xmlsoft -- libxml2	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML mixed content, causing a NULL dereference. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be used to crash the application. The highest threat from this vulnerability is to system availability.	2021-05-14	4.3	CVE-2021-3537 MISC FEDORA MLIST

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dedecms -- dedecms	A XSS Vulnerability in /uploads/dede/action_search.php in DedeCMS V5.7 SP2 allows an authenticated user to execute remote arbitrary code via the keyword parameter.	2021-05-15	3.5	CVE-2020-16632 MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The API of 'tf.raw_ops.SparseCross' allows combinations which would result in a 'CHECK'-failure and denial of service. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/3d782b7d47b1bf2ed32bd4a246d8d6cad4c903d/tensorflow/core/ops/sparse_cross_op.cc#L116) is tricked to consider a tensor of type 'tstring' which in fact contains integral elements. Fixing the type confusion by preventing mixing 'DT_STRING' and 'DT_INT64' types solves this issue. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29519 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a 'CHECK'-fail in 'tf.raw_ops.CTCGreedyDecoder'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1615440b17b364b875eb06f43d087381f1460a65/tensorflow/core/ops/ctc_decoder_op.cc#L50) has a 'CHECK_LT' inserted to validate some invariants. When this condition is false, the program aborts, instead of returning a valid error to the user. This abnormal termination can be weaponized in denial of service attacks. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29543 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Specifying a negative dense shape in `tf.raw_ops.SparseCountSparseOutput` results in a segmentation fault being thrown out from the standard library as `std::vector` invariants are broken. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/sparse_count_sparse_output_op.cc#L213) assumes the first element of the dense shape is always positive and uses it to initialize a `BatchedMap<T>` (i.e., `std::vector<absl::flat_hash_map<int64,T>>` (https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/sparse_count_sparse_output_op.cc#L213)). If the `shape` tensor has more than one element, `num_batches` is the first value in `shape`. Ensuring that the `dense_shape` argument is a valid tensor shape (that is, all elements are non-negative) solves this issue. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3.	2021-05-14	2.1	CVE-2021-29521 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can access data outside of bounds of heap allocated array in `tf.raw_ops.UnicodeEncode`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/472c1f12ad9063405737679d4f6b493094e1d36d/tensorflow/core/kernels/unicode_encode_op.cc#L122) assumes that the `input_value`/`input_splits` pair specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29559 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.RaggedTensorToTensor`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cece54f6a1977b/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L222) uses the same index to access two arrays in parallel. Since the user controls the shape of the input arguments, an attacker could trigger a heap OOB access when `parent_output_index` is shorter than `row_split`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29560 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ac328eaa3870491ababc147822cd04e91a790643/tensorflow/core/kernels/max_pool_grad_with_argmax_op.cc#L50) assumes that the `input_min` and `input_max` tensors have at least one element, as it accesses the first element in two arrays. If the tensors are empty, `flat<T>()` is an empty object, backed by an empty array. Hence, accessing even the 0th element is a read outside the bounds. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29569 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ef0c008ee84bad91ec6725ddc42091e19a30c10e/tensorflow/core/kernels/max_pool_grad_with_argmax_op.cc#L1017) uses the same value to index in two different arrays but there is no guarantee that the sizes are identical. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29570 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.Dequantize`, an attacker can trigger a read from outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/26003593aa94b1742f34dc22ce88a1e129502/tensorflow/core/kernels/dequantize_op.cc#L131) accesses the `min_range` and `max_range` tensors in parallel but fails to check that they have the same shape. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29582 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementations of the 'Minimum' and 'Maximum' TFLite operators can be used to read data outside of bounds of heap allocated objects, if any of the two input tensor arguments are empty. This is because the broadcasting implementation(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda204e7e7/tensorflow/lite/kernels/minimum.cc#L56) indexes in both tensors with the same index but does not validate that the index is within bounds. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29590 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of concatenation is vulnerable to an integer overflow issue(https://github.com/tensorflow/tensorflow/blob/7b7352a724b690b11bfaae2cd54bc3907daf6285/tensorflow/lite/kernels/concat.cc#L76). An attacker can craft a model such that the dimensions of one of the concatenation input overflow the values of 'int'. TFLite uses 'int' to represent tensor dimensions, whereas TF uses 'int64'. Hence, valid TF models can trigger an integer overflow when converted to TFLite format. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29601 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in 'tf.raw_ops.CTCLoss' allows an attacker to trigger an OOB read from heap. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick these commits on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29613 CONFIRM MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Calling 'tf.raw_ops.RaggedTensorToVariant' with arguments specifying an invalid ragged tensor results in a null pointer dereference. The implementation of 'RaggedTensorToVariant' operations(https://github.com/tensorflow/tensorflow/blob/904b3926ed1c6c70380d5313d282d248a776baa1/tensorflow/lite/kernels/ragged_tensor_to_variant.cc#L40) does not validate that the ragged tensor argument is non-empty. Since 'batched_ragged' contains no elements, 'batched_ragged.splits' is a null vector, thus 'batched_ragged.splits(0)' will result in dereferencing 'nullptr'. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29516 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can read data outside of bounds of heap allocated buffer in 'tf.raw_ops.QuantizeAndDequantizeV3'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/11ff7b0667e6490d7b5174aa6bf5e01b80e7720/tensorflow/lite/kernels/quantize_and_dequantize.cc#L117) does not validate the value of user supplied 'axis' attribute before using it to index in the array backing the 'input' argument. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29553 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. A malicious user could trigger a division by 0 in 'Conv3D' implementation. The implementation(https://github.com/tensorflow/tensorflow/blob/42033603003965bffa51ae171b51801565e002d/tensorflow/lite/kernels/conv.cc#L145) does a modulo operation based on user controlled input. Thus, when 'filter' has a 0 as the fifth element, this results in a division by 0. Additionally, if the shape of the two tensors is not valid, an Eigen assertion can be triggered, resulting in a program crash. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29517 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in converting sparse tensors to CSR Sparse matrices. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/800346f2c03a27e182dd4fba48295f65e7790739/tensorflow/core/kernels/sparse_to_csr_sparse_mat.cc#L450) does a double redirection to access an element of an array allocated on the heap. If the value at `indices(i, 0)` is such that `indices(i, 0) + 1` is outside the bounds of `csr_row_ptr`, this results in writing outside of bounds of heap allocated data. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29545 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The `tf.raw_ops.Conv3DBackprop` operations fail to validate that the input tensors are not empty. In turn, this would result in a division by 0. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a91bb59769f19146d5a0c20060244378e878f140/tensorflow/core/kernels/conv3d_backprop.cc#L450) does not check that the divisor used in computing the shard size is not zero. Thus, if attacker controls the input sizes, they can trigger a denial of service via a division by zero error. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29522 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.QuantizedConv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/00e9a4d67d76703fa1aee33dac582a1f307e0e2852/tensorflow/core/kernels/quantized_conv2d.cc#L259) does a division by a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29527 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a dereference of a null pointer in `tf.raw_ops.StringNGrams`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams.cc#L110) does not fully validate the `data_splits` argument. This would result in `ngrams_data` (https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams.cc#L110) to be a null pointer when the output would be computed to have 0 or negative size. Later writes to the output tensor would then cause a null pointer dereference. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29541 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.ImmutableConst` (https://www.tensorflow.org/api_docs/python/tf/raw_ops/ImmutableConst) with a `dtype` of `tf.resource` or `tf.variant` results in a segfault in the implementation as code assumes that the tensor contents are pure scalars. We have patched the issue in 4f663d4b8f0bec1b48da6fa091a7d29609980fa4 and will release TensorFlow 2.5.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved. If using `tf.raw_ops.ImmutableConst` in code, you can prevent the segfault by inserting a filter for the `dtype` argument.	2021-05-14	2.1	CVE-2021-29539 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a division by zero to occur in `Conv2DBackpropFilter`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd943f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv2d_backprop_filter.cc#L522) computes a divisor based on user provided data (i.e., the shape of the tensors given as arguments). If all shapes are empty then `work_unit_size` is 0. Since there is no check for this case before division, this results in a runtime exception, with potential to be abused for a denial of service. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29538 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a 'CHECK'-fail in 'tf.raw_ops.SparseConcat'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/b432a38fe0e1b4b904a6c222cbce794c39703e87/tensorflow/core/ops/sparse_ops_sparse_concat.cc#L188) uses a 'CHECK' operation which triggers when 'InitDims' (https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/ops/sparse_ops_sparse_concat.cc#L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use 'BuildTensorShapeBase' or 'AddDimWithStatus' to prevent 'CHECK'-failures in the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29534 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a 'CHECK' failure by passing an empty image to 'tf.raw_ops.DrawBoundingBoxes'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/ea34a18dc3f5c8d80a40ccca1404f343b5d55f91/tensorflow/core/ops/image_ops_image_draw_bounding_boxes.cc#L165) uses 'CHECK_*' assertions instead of 'OP_REQUIRES' to validate user controlled inputs. Whereas 'OP_REQUIRES' allows returning an error condition back to the user, the 'CHECK_*' macros result in a crash if the condition is false, similar to 'assert'. In this case, 'height' is 0 from the 'images' input. This results in 'max_box_row_clamp' being negative and the assertion being falsified, followed by aborting program execution. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29533 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a 'CHECK' fail in PNG encoding by providing an empty input tensor as the pixel data. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/ops/image_ops_image_png_encode.cc#L93) only validates that the total number of pixels in the image does not overflow. Thus, an attacker can send an empty matrix for encoding. However, if the tensor is empty, then the associated buffer is 'nullptr'. Hence, when calling 'png::WriteImageToBuffer' (https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/ops/image_ops_image_png_encode.cc#L349), the first argument (i.e., 'image.flat<T>().data()') is 'NULL'. This then triggers the 'CHECK_NOTNULL' in the first line of 'png::WriteImageToBuffer' (https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/ops/image_ops_image_png_encode.cc#L349). Since 'image' is null, this results in 'abort' being called after printing the stacktrace. Effectively, this allows an attacker to mount a denial of service attack. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29531 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in 'tf.raw_ops.QuantizedMul'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/5590e961ed4a23b4383920249121542021568526/tensorflow/core/ops/math_ops_quantized_mul.cc#L198) does a division by a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29526 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Passing invalid arguments (e.g., discovered via fuzzing) to 'tf.raw_ops.SparseCountSparseOutput' results in segfault. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29619 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/988087bd83f144af14087fe4feceeb2150193720526/tensorflow/core/ops/conv2d_impl.cc#L263) does a division by a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29526 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.AddManySparseToTensorsMap`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/ops/sparse_ops.cc#L188) uses a `CHECK` operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/ops/sparse_ops.cc#L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to prevent `CHECK`-failures in the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29523 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropFilter`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/496c2630e51c1a478f095b084329a6cd2253db9524/tensorflow/core/ops/conv2d_backprop.cc#L496) does a modulus operation where the divisor is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29524 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can force accesses outside the bounds of heap allocated arrays by passing in invalid tensor values to `tf.raw_ops.RaggedCross`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/efea03b38fb8d3b81762237dc85e579cc5fc6e87/tensorflow/core/ops/ragged_ops.cc#L487) lacks validation for the user supplied arguments. Each of the above branches call a helper function after accessing array elements via a `*_list[next_*]` pattern, followed by incrementing the `next_*` index. However, as there is no validation that the `next_*` values are in the valid range for the corresponding `*_list` arrays, this results in heap OOB reads. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	3.6	CVE-2021-29532 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow by passing crafted inputs to `tf.raw_ops.StringNGrams`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/ops/string_ops.cc#L185) fails to consider corner cases where input would be split in such a way that the generated tokens should only contain padding elements. If input is such that `num_tokens` is 0, then, for `data_start_index=0` (when left padding is present), the marked line would result in reading `data[-1]`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29542 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Passing a complex argument to `tf.transpose` at the same time as passing `conjugate=True` argument results in a crash. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29618 MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the implementation of `tf.raw_ops.RFFT`. Eigen code operating on an empty matrix can trigger on an assertion and will cause program termination. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29563 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.EditDistance`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/79865b542f9fddc9caeb255631f7c507f42023179504/tensorflow/core/ops/edit_distance_ops.cc#L159) has incomplete validation of the input parameters. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29564 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a segfault and denial of service via accessing data outside of bounds in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0bbbeb414dc0553d3ae71/tensorflow/core/ops/quantized_batch_norm_with_global_normalization.cc#L189) assumes the inputs are not empty. If any of these inputs is empty, `.flat<T>()` is an empty buffer, so accessing the element at index 0 is accessing data outside of bounds. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29543 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0bbbeb414dc0553d3ae71/tensorflow/core/ops/quantized_batch_norm_with_global_normalization.cc#L189) does not validate all constraints specified in the op's contract(https://www.tensorflow.org/api_docs/python/tf/raw_ops/QuantizedBatchNormWithGlobalNormalization). The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29548 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/ops/quantized_batch_norm_with_global_normalization.cc#L295) computes a modulo operation without validating that the divisor is not zero. Since `vector_num_elements` is determined based on input shapes(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/ops/quantized_batch_norm_with_global_normalization.cc#L544), a user can trigger scenarios where this quantity is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29549 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in 'tf.raw_ops.FractionalAvgPool'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/ops/avg_pool_grad.cc#L89) computes a divisor quantity by dividing two user controlled values. The user controls the values of 'input_size[i]' and 'pooling_ratio[i]' (via the 'value.shape()' and 'pooling_ratio' arguments). If the value in 'input_size[i]' is smaller than the 'pooling_ratio[i]', then the floor operation results in 'output_size[i]' being 0. The 'DCHECK_GT' line is a no-op outside of debug mode, so in released versions of TF this does not trigger. Later, these computed values are used as arguments(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/ops/avg_pool_grad.cc#L99) to 'GeneratePoolingSequence'(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/ops/avg_pool_grad.cc#L108). There, the first computation is a division in a modulo operation. Since 'output_length' can be 0, this results in runtime crashing. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29550 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of 'MatrixTriangularSolve'(https://github.com/tensorflow/tensorflow/blob/8cae746d8449c7dda5298327353d68613f16e798/tensorflow/core/ops/matrix_triangular_solve.cc#L240) fails to terminate kernel execution if one validation condition fails. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29551 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by controlling the values of 'num_segments' tensor argument for 'UnsortedSegmentJoin'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a2a607db15c7cd01d754d37e5448d72a13491bdb/tensorflow/core/ops/unsorted_segment_join.cc#L93) assumes that the 'num_segments' tensor is a valid scalar. Since the tensor is empty the 'CHECK' involved in '.scalar<T>()' that checks that the number of elements is exactly 1 will be invalidated and this would result in process termination. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29552 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in 'tf.raw_ops.DenseCountSparseOutput'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/eff014f3b2d8ef6141da30c806faf1c9292d4120c/tensorflow/core/ops/dense_count_sparse_output.cc#L127) computes a divisor value from user data but does not check that the result is 0 before doing the division. Since 'data' is given by the 'values' argument, 'num_batch_elements' is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, and TensorFlow 2.3.3, as these are also affected.	2021-05-14	2.1	CVE-2021-29554 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in 'tf.raw_ops.FusedBatchNorm'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/828f346274841fa7505f7020e88ca66c229257200/tensorflow/core/ops/fused_batch_norm.cc#L297) performs a division based on the last dimension of the 'x' tensor. Since this is controlled by the user, an attacker can trigger a denial of service. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29555 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in 'tf.raw_ops.Reverse'. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/36229ea9e9451dac14a8b1f4711cd35a2024a299/tensorflow/core/ops/rev.cc#L76) performs a division based on the first dimension of the tensor argument. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29556 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.SparseMatMul`. The division by 0 occurs deep in Eigen code because the `b` tensor is empty. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29557 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via `CHECK`-fail in `tf.strings.substr` with invalid arguments. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29617 MISC CONFIRM MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the implementation of `tf.raw_ops.IRFFT`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29562 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from `tf.raw_ops.LoadAndRemapMatrix`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cece54f6a1977b/tensorflow/L222) assumes that the `ckpt_path` is always a valid scalar. However, an attacker can send any other tensor as the first argument of `LoadAndRemapMatrix`. This would cause the rank `CHECK` in `scalar<T>()` to trigger and terminate the process. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29561 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.SparseDenseCwiseMul`, an attacker can trigger denial of service via `CHECK`-fails or accesses to outside the bounds of heap allocated data. Since the implementation(https://github.com/tensorflow/tensorflow/blob/38178a2f7a681a7835bb0912702a134bfe3b4d84/tensorflow/L80) only validates the rank of the input arguments but no constraints between dimensions(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SparseDenseCwiseMul), an attacker can abuse them to trigger internal `CHECK` assertions (and cause program termination, denial of service) or to write to memory outside of bounds of heap allocated tensor buffers. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29567 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in caused by an integer overflow in constructing a new tensor shape. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/0908c2f2397c099338b901b067f6495a5b96760b/tensorflow/L70) builds a dense shape without checking that the dimensions would not result in overflow. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/L188) uses a `CHECK` operation which triggers when `InitDims` (https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to prevent `CHECK`-failures in the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29584 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `ParseAttrValue` (https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3f09aa74ed79595/tensorflow/core/kernels/parse_attr_value.cc#L453) can be tricked into stack overflow due to recursion by giving in a specially crafted input. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29615 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseReshape` results in a denial of service based on a `CHECK`-failure. The implementation (https://github.com/tensorflow/tensorflow/blob/e87b51ce05c3eb172065a6ea5f484f563f225285/tensorflow/core/kernels/sparse_reshape.cc#L127) has no validation that the input arguments specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are the only affected versions.	2021-05-14	2.1	CVE-2021-29611 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite code for allocating `TFLiteIntArray`'s is vulnerable to an integer overflow issue (https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cd/tensorflow/lite/c/cor L27). An attacker can craft a model such that the `size` multiplier is so large that the return value overflows the `int` datatype and becomes negative. In turn, this results in invalid value being given to `malloc` (https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cd/tensorflow/lite/c/cor L52). In this case, `ret->size` would dereference an invalid pointer. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29605 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.SparseFillEmptyRows`. This is because of missing validation (https://github.com/tensorflow/tensorflow/blob/fdc82089d206e281c628a93771336bf87863d5e8/tensorflow/co L231) that was covered under a `TODO`. If the `dense_shape` tensor is empty, then `dense_shape_t.vec<>()` would cause a null pointer dereference in the implementation of the op. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29565 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `DepthwiseConv` TFLite operator is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e8330b225285/tensorflow/lite/ke L288). An attacker can craft a model such that `input`'s fourth dimension would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29607 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of hashtable lookup is vulnerable to a division by zero error (https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e8330b225285/tensorflow/lite/ke L115). An attacker can craft a model such that `values`'s first dimension would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29604 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.CTCBeamSearchDecoder`, an attacker can trigger denial of service via segmentation faults. The implementation (https://github.com/tensorflow/tensorflow/blob/a74768f8e4efbda4def9f16ee7e13c922825f2/tensorflow L79) fails to detect cases when the input tensor is empty and proceeds to read data from a null buffer. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29561 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalMaxPoolGrad` triggers an undefined behavior if one of the input tensors is empty. The code is also vulnerable to a denial of service attack as a `CHECK` condition becomes false and aborts the process. The implementation(https://github.com/tensorflow/tensorflow/blob/169054888d50ce488dfde9ca55d910b32a9f0d5b/tensorflow/core/ops/fractional_max_pool_grad.cc#L118) fails to validate that input and output tensors are not empty and are of the same rank. Each of these unchecked assumptions is responsible for the above issues. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29580 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.ReverseSequence` allows for stack overflow and/or `CHECK`-fail based denial of service. The implementation(https://github.com/tensorflow/tensorflow/blob/5b3b071975e01f0d250c928b2a8f901cd53b90a7/tensorflow/core/ops/reverse_sequence.cc#L118) fails to validate that `seq_dim` and `batch_dim` arguments are valid. Negative values for `seq_dim` can result in stack overflow or `CHECK`-failure, depending on the version of Eigen code used to implement the operation. Similar behavior can be exhibited by invalid values of `batch_dim`. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29575 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` is vulnerable to a division by 0. The implementation(https://github.com/tensorflow/tensorflow/blob/279bab6efa22752a2827621b7ed6567201339b7/tensorflow/core/ops/max_pool_grad_with_argmax.cc#L1034) fails to validate that the batch dimension of the tensor is non-zero, before dividing by this quantity. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29576 CONFIRM MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.SdcaOptimizer` triggers undefined behavior due to dereferencing a null pointer. The implementation(https://github.com/tensorflow/tensorflow/blob/60a45c8b6192a4699f2e2709a2645a751d435cc3/tensorflow/core/ops/sdca_optimizer.cc#L163) does not validate that the user supplied arguments satisfy all constraints expected by the op(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SdcaOptimizer). The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.	2021-05-14	2.1	CVE-2021-29572 MISC CONFIRM
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.QuantizeAndDequantizeV4Grad`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/95078c145b5a7a43ee046144005f733092756ab5/tensorflow/core/ops/quantize_and_dequantize_v4_grad.cc#L306) does not validate the rank of the `input_*` tensors. In turn, this results in the tensors being passed as they are to `QuantizeAndDequantizePerChannelGradientImpl` (https://github.com/tensorflow/tensorflow/blob/95078c145b5a7a43ee046144005f733092756ab5/tensorflow/core/ops/quantize_and_dequantize_per_channel_gradient_impl.cc#L306). However, the `vec<T>` method, requires the rank to 1 and triggers a `CHECK` failure otherwise. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2 as this is the only other affected version.	2021-05-14	2.1	CVE-2021-29544 MISC CONFIRM
haml-coffee_project -- haml-coffee	haml-coffee is a JavaScript templating solution. haml-coffee mixes pure template data with engine configuration options through the Express render API. More specifically, haml-coffee supports overriding a series of HTML helper functions through its configuration options. A vulnerable application that passes user controlled request objects to the haml-coffee template engine may introduce RCE vulnerabilities. Additionally control over the escapeHtml parameter through template configuration pollution ensures that haml-coffee would not sanitize template inputs that may result in reflected Cross Site Scripting attacks against downstream applications. There is currently no fix for these issues as of the publication of this CVE. The latest version of haml-coffee is currently 1.14.1. For complete details refer to the referenced GHSL-2021-025.	2021-05-14	3.5	CVE-2021-32818 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- qradar_user_behavior_analytics	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 195999.	2021-05-14	2.1	CVE-2021-20391 XF CONFIRM
laobancms -- laobancms	Cross Site Scripting (XSS) in LAOBANCMS v2.0 allows remote attackers to execute arbitrary code by injecting commands into the "Homepage Introduction" field of component "admin/info.php?shuyu".	2021-05-14	3.5	CVE-2020-18167 MISC
pickplugins -- accordion	The tab GET parameter of the settings page is not sanitised or escaped when being output back in an HTML attribute, leading to a reflected XSS issue.	2021-05-14	3.5	CVE-2021-24283 CONFIRM
wpuslugi -- rss_for_yandex_turbo	The RSS for Yandex Turbo WordPress plugin before 1.30 did not properly sanitise the user inputs from its $\text{D}_i\text{N}\ddot{\text{D}}\mu\text{N},\text{N}\ddot{\text{D}}\text{D},\text{D}^{\circ}\text{D}$, settings tab before outputting them back in the page, leading to authenticated stored Cross-Site Scripting issues	2021-05-14	3.5	CVE-2021-24277 CONFIRM
yfcmf -- yfcmf	In YFCMF v2.3.1, there is a stored XSS vulnerability in the comments section of the news page.	2021-05-14	3.5	CVE-2020-23689 MISC

[Back to top](#)

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acymailing -- acymailing	When subscribing using AcyMailing, the 'redirect' parameter isn't properly sanitized. Turning the request from POST to GET, an attacker can craft a link containing a potentially malicious landing page and send it to the victim.	2021-05-17	not yet calculated	CVE-2021-24288 CONFIRM
admidio -- admidio	Admidio is a free, open source user management system for websites of organizations and groups. In Admidio before version 4.0.4, there is an authenticated RCE via .phar file upload. A php web shell can be uploaded via the Documents & Files upload feature. Someone with upload permissions could rename the php shell with a .phar extension, visit the file, triggering the payload for a reverse/bind shell. This can be mitigated by excluding a .phar file extension to be uploaded (like you did with .php .phtml .php5 etc). The vulnerability is patched in version 4.0.4.	2021-05-20	not yet calculated	CVE-2021-32630 MISC CONFIRM MISC
adminer -- adminer	Adminer is open-source database management software. A cross-site scripting vulnerability in Adminer versions 4.6.1 to 4.8.0 affects users of MySQL, MariaDB, PostgreSQL and SQLite. XSS is in most cases prevented by strict CSP in all modern browsers. The only exception is when Adminer is using a 'pdo_' extension to communicate with the database (it is used if the native extensions are not enabled). In browsers without CSP, Adminer versions 4.6.1 to 4.8.0 are affected. The vulnerability is patched in version 4.8.1. As workarounds, one can use a browser supporting strict CSP or enable the native PHP extensions (e.g. 'mysqli') or disable displaying PHP errors ('display_errors').	2021-05-19	not yet calculated	CVE-2021-29625 MISC MISC CONFIRM
arm -- trustzone_cryptocell	The elliptic curve cryptography (ECC) hardware accelerator, part of the ARM® TrustZone® CryptoCell 310, contained in the NordicSemiconductor nRF52840 through 2021-03-29 has a non-constant time ECDSA implementation. This allows an adversary to recover the private ECC key used during an ECDSA operation.	2021-05-21	not yet calculated	CVE-2021-29415 MISC MISC
bitdefender -- endpoint_security_tools	An Improper Access Control vulnerability in the logging component of Bitdefender Endpoint Security Tools for Windows versions prior to 6.6.23.320 allows a regular user to learn the scanning exclusion paths. This issue was discovered during external security research.	2021-05-18	not yet calculated	CVE-2020-15279 CONFIRM
bitdefender -- gravityzone_business_security	Uncontrolled Search Path Element vulnerability in the openssl component as used in Bitdefender GravityZone Business Security allows an attacker to load a third party DLL to elevate privileges. This issue affects Bitdefender GravityZone Business Security versions prior to 6.6.23.329.	2021-05-18	not yet calculated	CVE-2021-3423 CONFIRM
bludit -- bludit	A file upload vulnerability was discovered in the file path /bl-plugins/backup/plugin.php on Bludit version 3.12.0. If an attacker is able to gain Administrator rights they will be able to use unsafe plugins to upload a backup file and control the server.	2021-05-21	not yet calculated	CVE-2020-23765 MISC
bmc -- remedy_mid_tier_9.1sp3	BMC Remedy 9.1SP3 is affected by authenticated code execution. Authenticated users that have the right to create reports can use BIRT templates to run code.	2021-05-19	not yet calculated	CVE-2017-17677 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bmc -- remedy_mid_tier_9.1sp3	BMC Remedy Mid Tier 9.1SP3 is affected by cross-site scripting (XSS). A DOM-based cross-site scripting vulnerability was discovered in a legacy utility.	2021-05-19	not yet calculated	CVE-2017-17678 MISC MISC MISC MISC
bmc -- remedy_mid_tier_9.1sp3	BMC Remedy Mid Tier 9.1SP3 is affected by remote and local file inclusion. Due to the lack of restrictions on what can be targeted, the system can be vulnerable to attacks such as system fingerprinting, internal port scanning, Server Side Request Forgery (SSRF), or remote code execution (RCE).	2021-05-19	not yet calculated	CVE-2017-17674 MISC MISC MISC MISC
bmc -- remedy_mid_tier_9.1sp3	BMC Remedy Mid Tier 9.1SP3 is affected by log hijacking. Remote logging can be accessed by unauthenticated users, allowing for an attacker to hijack the system logs. This data can include user names and HTTP data.	2021-05-19	not yet calculated	CVE-2017-17675 MISC MISC MISC MISC
boostnote -- boostnote	In Boostnote 0.12.1, exporting to PDF contains opportunities for XSS attacks.	2021-05-18	not yet calculated	CVE-2020-19924 MISC
bounty_castle -- bounty_castle	Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.	2021-05-20	not yet calculated	CVE-2020-15522 MISC MISC MISC
centos -- web+panel	The unprivileged user portal part of CentOS Web Panel is affected by a SQL Injection via the 'idsession' HTTP POST parameter.	2021-05-18	not yet calculated	CVE-2021-31316 MISC
centos -- web_panel	The unprivileged user portal part of CentOS Web Panel is affected by a Command Injection vulnerability leading to root Remote Code Execution.	2021-05-18	not yet calculated	CVE-2021-31324 MISC
cflow -- cflow	Use-after-Free vulnerability in cflow 1.6 in the void call(char *name, int line) function at src/parser.c, which could cause a denial of service via the pointer variable caller->callee.	2021-05-18	not yet calculated	CVE-2020-23856 MISC MISC
cisco -- dna_spaces_connector	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	not yet calculated	CVE-2021-1559 CISCO
cisco -- dna_spaces_connector	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	not yet calculated	CVE-2021-1560 CISCO
cisco -- dna_spaces_connector	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.	2021-05-22	not yet calculated	CVE-2021-1557 CISCO
cisco -- dna_spaces_connector	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.	2021-05-22	not yet calculated	CVE-2021-1558 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- finesse	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerability is known as an open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites.	2021-05-22	not yet calculated	CVE-2021-1358 CISCO
cisco -- finesse	Multiple vulnerabilities in the web-based management interface of Cisco Finesse could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities by injecting malicious code into the web-based management interface and persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. An attacker needs valid administrator credentials to inject the malicious script code.	2021-05-22	not yet calculated	CVE-2021-1254 CISCO
cisco -- modeling_labs	A vulnerability in the web UI of Cisco Modeling Labs could allow an authenticated, remote attacker to execute arbitrary commands with the privileges of the web application on the underlying operating system of an affected Cisco Modeling Labs server. This vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected server. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the web application, virl2, on the underlying operating system of the affected server. To exploit this vulnerability, the attacker must have valid user credentials on the web UI.	2021-05-22	not yet calculated	CVE-2021-1531 CISCO
cisco -- multiple_products	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user.	2021-05-22	not yet calculated	CVE-2021-1306 CISCO
cisco -- prime_infrastructure_and_evolved_programmable_network_manager	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition.	2021-05-22	not yet calculated	CVE-2021-1487 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1549 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1555 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1551 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1552 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1548 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1553 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1554 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1550 CISCO
cisco -- small_business	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	not yet calculated	CVE-2021-1547 CISCO
cmswing -- cmswing	There is a cross site scripting vulnerability on CmsWing 1.3.7. This vulnerability (stored XSS) is triggered when visitors access the article module.	2021-05-17	not yet calculated	CVE-2020-24993 MISC
cmswing -- cmswing	There is a cross site scripting vulnerability on CmsWing 1.3.7. This vulnerability (stored XSS) is triggered when an administrator accesses the content management module.	2021-05-17	not yet calculated	CVE-2020-24992 MISC
concerto -- concerto	Persistent cross-site scripting (XSS) in the web interface of Concerto through 2.3.6 allows an unauthenticated remote attacker to introduce arbitrary JavaScript by injecting an XSS payload into the First Name or Last Name parameter upon registration. When a privileged user attempts to delete the account, the XSS payload will be executed.	2021-05-19	not yet calculated	CVE-2021-31930 MISC MISC
couchbase_server -- couchbase_server	An issue was discovered in Couchbase Server 6.x through 6.6.1. The Couchbase Server UI is insecurely logging session cookies in the logs. This allows for the impersonation of a user if the log files are obtained by an attacker before a session cookie expires.	2021-05-19	not yet calculated	CVE-2021-27924 MISC MISC
couchbase_server -- couchbase_server	In the Query Engine in Couchbase Server 6.5.x and 6.6.x through 6.6.1, Common Table Expression queries were not correctly checking the user's permissions, allowing read-access to resources beyond what those users were explicitly allowed to access.	2021-05-19	not yet calculated	CVE-2021-31158 MISC MISC
couchbase_server -- couchbase_server	An issue was discovered in Couchbase Server 6.5.x and 6.6.x through 6.6.1. When using the View Engine and Auditing is enabled, a crash condition can (depending on a race condition) cause an internal user with administrator privileges, @ns_server, to have its credentials leaked in cleartext in the ns_server.info.log file.	2021-05-19	not yet calculated	CVE-2021-27925 MISC MISC
couchbase_server -- couchbase_server	An issue was discovered in Couchbase Server 5.x and 6.x through 6.6.1 and 7.0.0 Beta. Incorrect commands to the REST API can result in leaked authentication information being stored in cleartext in the debug.log and info.log files, and is also shown in the UI visible to administrators.	2021-05-19	not yet calculated	CVE-2021-25644 MISC MISC
d-link -- dir-842_routers	An authentication brute-force protection mechanism bypass in telnetd in D-Link Router model DIR-842 firmware version 3.0.2 allows a remote attacker to circumvent the anti-brute-force cool-down delay period via a timing-based side-channel attack	2021-05-17	not yet calculated	CVE-2021-27342 MISC MISC CONFIRM
dell -- emc_xtremio	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerability, leading to a privileged victim application user being tricked into sending state-changing requests to the vulnerable application, causing unintended server operations.	2021-05-21	not yet calculated	CVE-2021-21549 CONFIRM
dell -- wyse_windows_embedded_system	Dell Wyse Windows Embedded System versions WIE10 LTSC 2019 and earlier contain an improper authorization vulnerability. A local authenticated malicious user with low privileges may potentially exploit this vulnerability to bypass the restricted environment and perform unauthorized actions on the affected system.	2021-05-21	not yet calculated	CVE-2021-21552 CONFIRM
delta_industrial_automation -- cncsoft_screeditor	Delta Industrial Automation CNCSoft ScreenEditor Versions 1.01.28 (with ScreenEditor Version 1.01.2) and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.	2021-05-16	not yet calculated	CVE-2021-22668 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dns-package -- dns-package	This affects the package dns-packet before 5.2.2. It creates buffers with allocUnsafe and does not always fill them before forming network packets. This can expose internal application memory over unencrypted network when querying crafted invalid domain names.	2021-05-20	not yet calculated	CVE-2021-23386 MISC MISC MISC MISC
doracms -- doracms	Weak Encoding for Password in DoraCMS v2.1.1 and earlier allows attackers to obtain sensitive information as it does not use a random salt or IV for its AES-CBC encryption, causes password encrypted for users to be susceptible to dictionary attacks.	2021-05-20	not yet calculated	CVE-2020-18220 MISC
draeger -- x-dock_firmware	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker.	2021-05-20	not yet calculated	CVE-2021-28111 MISC CONFIRM MISC
draeger -- x-dock_firmware	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker.	2021-05-20	not yet calculated	CVE-2021-28112 MISC CONFIRM
drupal -- core_workspaces	Access bypass vulnerability in of Drupal Core Workspaces allows an attacker to access data without correct permissions. The Workspaces module doesn't sufficiently check access permissions when switching workspaces, leading to an access bypass vulnerability. An attacker might be able to see content before the site owner intends people to see the content. This vulnerability is mitigated by the fact that sites are only vulnerable if they have installed the experimental Workspaces module. This issue affects Drupal Core 8.8.X versions prior to 8.8.10; 8.9.X versions prior to 8.9.6; 9.0.X versions prior to 9.0.6.	2021-05-17	not yet calculated	CVE-2020-13667 CONFIRM
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data.	2021-05-20	not yet calculated	CVE-2021-27465 MISC
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information.	2021-05-20	not yet calculated	CVE-2021-27463 MISC
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access.	2021-05-20	not yet calculated	CVE-2021-27457 MISC
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs.	2021-05-20	not yet calculated	CVE-2021-27461 MISC
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information.	2021-05-20	not yet calculated	CVE-2021-27467 MISC
emerson -- rosemont_x-stream_gas_analyzer	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code.	2021-05-20	not yet calculated	CVE-2021-27459 MISC
emissary -- emissary	Emissary is a distributed, peer-to-peer, data-driven workflow framework. Emissary 6.4.0 is vulnerable to Unsafe Deserialization of post-authenticated requests to the [WorkspaceClient.Enqueue.action] (https://github.com/NationalSecurityAgency/emissary/blob/30c54ef162021621023604a929939f950068332/src/main/java) REST endpoint. This issue may lead to post-auth Remote Code Execution. This issue has been patched in version 6.5.0. As a workaround, one can disable network access to Emissary from untrusted sources.	2021-05-20	not yet calculated	CVE-2021-32634 CONFIRM MISC
emlog -- emlog	Cross Site Scripting (XSS) in emlog v6.0.0 allows remote attackers to execute arbitrary code by adding a crafted script as a link to a new blog post.	2021-05-17	not yet calculated	CVE-2020-18194 MISC
envoy -- envoy	An issue was discovered in Envoy 1.14.0. There is a remotely exploitable crash for HTTP2 Metadata, because an empty METADATA map triggers a Reachable Assertion.	2021-05-20	not yet calculated	CVE-2021-29258 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoy -- envoy	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable NULL pointer dereference and crash in TLS when an unknown TLS alert code is received.	2021-05-20	not yet calculated	CVE-2021-28683 MISC MISC MISC
envoy -- envoy	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable integer overflow in which a very large grpc-timeout value leads to unexpected timeout calculations.	2021-05-20	not yet calculated	CVE-2021-28682 MISC MISC MISC
epic_games -- psyonix_rocket_league	Epic Games / Psyonix Rocket League <=1.95 is affected by Buffer Overflow. Stack-based buffer overflow occurs when Rocket League handles UPK object files that can result in code execution and denial of service scenario.	2021-05-18	not yet calculated	CVE-2021-32238 MISC MISC MISC
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An inefficient algorithm (quadratic complexity) was found in Exiv2 versions v0.27.3 and earlier. The inefficient algorithm is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.4. Note that this bug is only triggered when <code>_writing_</code> the metadata, which is a less frequently used Exiv2 operation than <code>_reading_</code> the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as <code>'rm'</code> .	2021-05-17	not yet calculated	CVE-2021-32617 MISC CONFIRM
fastify-csrf -- fastify-csrf	fastify-csrf is an open-source plugin helps developers protect their Fastify server against CSRF attacks. Versions of fastify-csrf prior to 3.1.0 have a "double submit" mechanism using cookies with an application deployed across multiple subdomains, e.g. "heroku"-style platform as a service. Version 3.1.0 of the fastify-csrf fixes it. the vulnerability. The user of the module would need to supply a <code>'userInfo'</code> when generating the CSRF token to fully implement the protection on their end. This is needed only for applications hosted on different subdomains.	2021-05-19	not yet calculated	CVE-2021-29624 MISC MISC MISC CONFIRM MISC MISC
fedora_project -- fedora_project	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package or compromise an RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is to data integrity. This flaw affects RPM versions before 4.17.0-alpha.	2021-05-19	not yet calculated	CVE-2021-3421 MISC FEDORA FEDORA FEDORA
ffjpeg -- ffjpeg	A heap based buffer overflow vulnerability exists in ffjpeg through 2020-07-02 in the <code>jif_decode(void *ctxt, BMP *pb)</code> function at <code>ffjpeg/src/jif.c</code> (line 544 & line 545), which could cause a denial of service by submitting a malicious jpeg image.	2021-05-18	not yet calculated	CVE-2020-23852 MISC
ffjpeg -- ffjpeg	A stack-based buffer overflow vulnerability exists in ffjpeg through 2020-07-02 in the <code>jif_decode(void *ctxt, BMP *pb)</code> function at <code>ffjpeg/src/jif.c:513:28</code> , which could cause a denial of service by submitting a malicious jpeg image.	2021-05-18	not yet calculated	CVE-2020-23851 MISC
firely -- spark	Firely/Incendi Spark before 1.5.5-r4 lacks Content-Disposition headers in certain situations, which may cause crafted files to be delivered to clients such that they are rendered directly in a victim's web browser.	2021-05-14	not yet calculated	CVE-2021-32054 CONFIRM CONFIRM CONFIRM
flask -- flask	The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an independently maintained version of Flask-Security based on the 3.0.0 version of Flask-Security. All versions of Flask-Security-Too allow redirects after many successful views (e.g. <code>/login</code>) by honoring the <code>?next</code> query param. There is code in FS to validate that the url specified in the next parameter is either relative OR has the same netloc (network location) as the requesting URL. This check utilizes Python's <code>urlsplit</code> library. However many browsers are very lenient on the kind of URL they accept and 'fill in the blanks' when presented with a possibly incomplete URL. As a concrete example - setting <code>http://login?next=\\github.com</code> will pass FS's relative URL check however many browsers will gladly convert this to <code>http://github.com</code> . Thus an attacker could send such a link to an unwitting user, using a legitimate site and have it redirect to whatever site they want. This is considered a low severity due to the fact that if Werkzeug is used (which is very common with Flask applications) as the WSGI layer, it by default ALWAYS ensures that the Location header is absolute - thus making this attack vector mute. It is possible for application writers to modify this default behavior by setting the <code>'autocorrect_location_header=False'</code> .	2021-05-17	not yet calculated	CVE-2021-32618 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the browseForDoc function. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13523.	2021-05-21	not yet calculated	CVE-2021-31473 MISC MISC
fusionpbx -- fusionpbx	Directory Traversal vulnerability in FusionPBX 4.5.7, which allows a remote malicious user to delete folders on the system via the folder variable to app/edit/folderdelete.php.	2021-05-20	not yet calculated	CVE-2020-21057 MISC MISC
fusionpbx -- fusionpbx	Directory Traversal vulnerability exists in FusionPBX 4.5.7, which allows a remote malicious user to create folders via the folder variable to app/edit/foldernew.php.	2021-05-20	not yet calculated	CVE-2020-21056 MISC MISC
fusionpbx -- fusionpbx	Cross Site Scripting (XSS) vulnerability in FusionPBX 4.5.7 allows remote malicious users to inject arbitrary web script or HTML via an unsanitized "f" variable in app/lvars/lvars_textarea.php.	2021-05-20	not yet calculated	CVE-2020-21054 MISC MISC
fusionpbx -- fusionpbx	A Directory Traversal vulnerability exists in FusionPBX 4.5.7 allows malicious users to rename any file of the system via the (1) folder, (2) filename, and (3) newfilename variables in app/edit/filename.php.	2021-05-20	not yet calculated	CVE-2020-21055 MISC MISC
fusionpbx -- fusionpbx	Cross Site Scripting (XSS) vulnerability exists in FusionPBX 4.5.7 allows remote malicious users to inject arbitrary web script or HTML via an unsanitized "query_string" variable in app/devices/device_imports.php.	2021-05-20	not yet calculated	CVE-2020-21053 MISC MISC
github -- enterprise_server	A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. All permissions being granted would properly be shown during the first authorization, but in certain circumstances, if the user revisits the authorization flow after the GitHub App has configured additional user-level permissions, those additional permissions may not be shown, leading to more permissions being granted than the user potentially intended. This vulnerability affected GitHub Enterprise Server 3.0.x prior to 3.0.7 and 2.22.x prior to 2.22.13. It was fixed in versions 3.0.7 and 2.22.13. This vulnerability was reported via the GitHub Bug Bounty program.	2021-05-14	not yet calculated	CVE-2021-22866 CONFIRM CONFIRM
gnu_libredwg -- gnu_libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_handles ../../src/decode.c:2637.	2021-05-17	not yet calculated	CVE-2020-21831 MISC MISC
gnu_libredwg -- gnu_libredwg	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via output_TEXT ../../programs/dwg2SVG.c:114.	2021-05-17	not yet calculated	CVE-2020-21813 MISC MISC MISC
gnu_libredwg -- gnu_libredwg	GNU LibreDWG 0.10 is affected by: memcpy-param-overlap. The impact is: execute arbitrary code (remote). The component is: read_2004_section_header ../../src/decode.c:2580.	2021-05-17	not yet calculated	CVE-2020-21844 MISC MISC
gnu_libredwg -- gnu_libredwg	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2379.	2021-05-17	not yet calculated	CVE-2020-21827 MISC MISC
halo -- halo	Cross Site Scripting (XSS) vulnerability in Halo 1.1.3 via post publish components in the manage panel, which lets a remote malicious user execute arbitrary code.	2021-05-20	not yet calculated	CVE-2020-21345 MISC
hedgedoc -- hedgedoc	HedgeDoc is a platform to write and share markdown. HedgeDoc before version 1.8.2 is vulnerable to a cross-site scripting attack using the YAML-metadata of a note. An attacker with write access to a note can embed HTML tags in the Open Graph metadata section of the note, resulting in the frontend rendering the script tag as part of the <head> section. Unless your instance prevents guests from editing notes, this vulnerability allows unauthenticated attackers to inject JavaScript into notes that allow guest edits. If your instance prevents guests from editing notes, this vulnerability allows authenticated attackers to inject JavaScript into any note pages they have write-access to. This vulnerability is patched in version 1.8.2. As a workaround, one can disable guest edits until the next update.	2021-05-19	not yet calculated	CVE-2021-29503 MISC CONFIRM MISC
hewlett_packard_enterprises -- laser_jet_products	A potential buffer overflow in the software drivers for certain HP LaserJet products and Samsung product printers could lead to an escalation of privilege.	2021-05-20	not yet calculated	CVE-2021-3438 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hirschmann -- hios	Hirschmann HiOS 07.1.01, 07.1.02, and 08.1.00 through 08.5.xx and HiSecOS 03.3.00 through 03.5.01 allow remote attackers to change the credentials of existing users.	2021-05-17	not yet calculated	CVE-2021-27734 MISC
homee -- brain_cube	The USB firmware update script of homee Brain Cube v2 (2.28.2 and 2.28.4) devices allows an attacker with physical access to install compromised firmware. This occurs because of insufficient validation of the firmware image file and can lead to code execution on the device.	2021-05-20	not yet calculated	CVE-2020-24395 MISC MISC
homee -- brain_cube	homee Brain Cube v2 (2.28.2 and 2.28.4) devices have sensitive SSH keys within downloadable and unencrypted firmware images. This allows remote attackers to use the support server as a SOCKS proxy.	2021-05-20	not yet calculated	CVE-2020-24396 MISC MISC
hongcms -- hongcms	Path Traversal in HongCMS v4.0.0 allows remote attackers to view, edit, and delete arbitrary files via a crafted POST request to the component "/hcms/admin/index.php/language/ajax."	2021-05-18	not yet calculated	CVE-2020-18178 MISC
htmlly -- htmlly	An arbitrary file deletion vulnerability was discovered on htmlly v2.7.5 which allows remote attackers to use any absolute path to delete any file in the server should they gain Administrator privileges.	2021-05-21	not yet calculated	CVE-2020-23766 MISC
ibm -- cloud_pak	IBM Cloud Pak for Multicloud Management prior to 2.3 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 188902.	2021-05-19	not yet calculated	CVE-2020-4765 CONFIRM XF
ibm -- control_center	IBM Control Center 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198761.	2021-05-19	not yet calculated	CVE-2021-20528 XF CONFIRM
ibm -- control_center	IBM Control Center 6.2.0.0 could allow a user to obtain sensitive version information that could be used in further attacks against the system. IBM X-Force ID: 198763.	2021-05-19	not yet calculated	CVE-2021-20529 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism. IBM X-Force ID: 201775.	2021-05-17	not yet calculated	CVE-2021-29747 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be used in further attacks against the system. IBM X-Force ID: 199918.	2021-05-21	not yet calculated	CVE-2021-29681 XF CONFIRM
ibm -- maximo_asset_manager	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195522.	2021-05-19	not yet calculated	CVE-2021-20374 CONFIRM XF
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 connects to a MongoDB server. MongoDB, a document-oriented database system, is listening on the remote port, and it is configured to allow connections without password authentication. A remote attacker can gain unauthorized access to the database. IBM X-Force ID: 184600.	2021-05-17	not yet calculated	CVE-2020-4669 CONFIRM XF
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 connects to a Redis server. The Redis server, an in-memory data structure store, running on the remote host is not protected by password authentication. A remote attacker can exploit this to gain unauthorized access to the server. IBM X-Force ID: 186401.	2021-05-17	not yet calculated	CVE-2020-4670 CONFIRM XF
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 200102.	2021-05-20	not yet calculated	CVE-2021-29688 XF CONFIRM CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253.	2021-05-20	not yet calculated	CVE-2021-29692 XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015	2021-05-20	not yet calculated	CVE-2021-29686 XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252.	2021-05-20	not yet calculated	CVE-2021-29691 XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018	2021-05-20	not yet calculated	CVE-2021-29687 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199997	2021-05-20	not yet calculated	CVE-2021-29682 CONFIRM XF
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998.	2021-05-20	not yet calculated	CVE-2021-29683 CONFIRM XF
ibm -- spectrum_scale	IBM Spectrum Scale 1.1.1.0 through 1.1.8.4 Transparent Cloud Tiering could allow a remote attacker to obtain sensitive information, caused by the leftover files after configuration. IBM X-Force ID: 190298.	2021-05-20	not yet calculated	CVE-2020-4850 XF CONFIRM
ibm -- sterling_b2b_integrator_standard+edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5, 6.0.0.0 through 6.0.3.3, and 6.1.0.0 through 6.1.0.2 could allow an authenticated user to view pages they should not have access to due to improper authorization control.	2021-05-19	not yet calculated	CVE-2020-4646 XF CONFIRM
intelbras -- router_rf_301k_firmware	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of security mechanisms for token protection and unsafe inputs and modules.	2021-05-17	not yet calculated	CVE-2021-32403 MISC
intelbras -- router_rf_301k_firmware	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of validation and insecure configurations in inputs and modules.	2021-05-17	not yet calculated	CVE-2021-32402 MISC
invoiceplane -- invoiceplane	InvoicePlane 1.5.11 doesn't have any rate-limiting for password reset and the reset token is generated using a weak mechanism that is predictable.	2021-05-17	not yet calculated	CVE-2021-29023 MISC
invoiceplane -- invoiceplane	In InvoicePlane 1.5.11 a misconfigured web server allows unauthenticated directory listing and file download. Allowing an attacker to directory traversal and download files suppose to be private without authentication.	2021-05-17	not yet calculated	CVE-2021-29024 MISC
koa-remove-trailing-slashes -- koa-remove-trailing-slashes	The package koa-remove-trailing-slashes before 2.0.2 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable endpoint (such as https://example.com/attacker.example/). The vulnerable code is in index.js::removeTrailingSlashes(), as the web server uses relative URLs instead of absolute URLs.	2021-05-17	not yet calculated	CVE-2021-23384 MISC MISC
konawiki2 -- konawiki2	SQL injection vulnerability in the KonaWiki2 versions prior to 2.2.4 allows remote attackers to execute arbitrary SQL commands and to obtain/alter the information stored in the database via unspecified vectors.	2021-05-20	not yet calculated	CVE-2021-20720 MISC MISC
konawiki2 -- konawiki2	KonaWiki2 versions prior to 2.2.4 allows a remote attacker to upload arbitrary files via unspecified vectors. If the file contains PHP scripts, arbitrary code may be executed.	2021-05-20	not yet calculated	CVE-2021-20721 MISC MISC
libdnf -- libdnf	A flaw was found in libdnf's signature verification functionality in versions before 0.60.1. This flaw allows an attacker to achieve code execution if they can alter the header information of an RPM package and then trick a user or system into installing it. The highest risk of this vulnerability is to confidentiality, integrity, as well as system availability.	2021-05-19	not yet calculated	CVE-2021-3445 FEDORA MISC FEDORA
libredwg -- libredwg	A heap-based buffer overflow vulnerability exists in LibreDWG 0.10.1 via the read_system_page function at libredwg-0.10.1/src/decode_r2007.c:666:5, which causes a denial of service by submitting a dwg file.	2021-05-18	not yet calculated	CVE-2020-23861 MISC
libsolv -- libsolv	Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver *testcase_read(Pool *pool, FILE *fp, const char *testcase, Queue *job, char **resultlp, int *resultflagsp function at src/testcase.c: line 2334, which could cause a denial of service	2021-05-18	not yet calculated	CVE-2021-3200 MISC MISC
libwebp -- applyfilter	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ApplyFilter. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2018-25010 MISC
libwebp -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A use-after-free was found due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	not yet calculated	CVE-2020-36329 MISC
libwebp -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	not yet calculated	CVE-2020-36328 MISC
libwebp -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkAssignData. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2020-36331 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libwebp -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkVerifyAndAssign. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2020-36330 MISC
libwebp -- libwebp	A flaw was found in libwebp in versions before 1.0.1. When reading a file libwebp allocates an excessive amount of memory. The highest threat from this vulnerability is to the service availability.	2021-05-21	not yet calculated	CVE-2020-36332 MISC
libwebp -- putle16	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow was found in PutLE16(). The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	not yet calculated	CVE-2018-25011 MISC
libwebp -- webpmuxcreateinternal	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2018-25009 MISC
libwebp -- webpmuxcreateinternal	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2018-25012 MISC
libwebp -- readsymbol	A flaw was found in libwebp in versions before 1.0.1. An uninitialized variable is used in function ReadSymbol. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	not yet calculated	CVE-2018-25014 MISC
libwebp -- shiftbytes	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ShiftBytes. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	not yet calculated	CVE-2018-25013 MISC
libxml2 -- libxml2	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability.	2021-05-18	not yet calculated	CVE-2021-3518 FEDORA MLIST MISC
libxml2 -- libxml2	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application.	2021-05-19	not yet calculated	CVE-2021-3517 MISC FEDORA MLIST
libyang -- libyang	In function read_yin_leaf() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the operation of retval->ext[r]->flags that results in a crash.	2021-05-20	not yet calculated	CVE-2021-28906 CONFIRM
libyang -- libyang	In function read_yin_container() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the operation of retval->ext[r]->flags that results in a crash.	2021-05-20	not yet calculated	CVE-2021-28902 CONFIRM
libyang -- libyang	A stack overflow in libyang <= v1.0.225 can cause a denial of service through function lyxml_parse_mem(). lyxml_parse_elem() function will be called recursively, which will consume stack space and lead to crash.	2021-05-20	not yet calculated	CVE-2021-28903 CONFIRM
libyang -- libyang	In function ext_get_plugin() in libyang <= v1.0.225, it doesn't check whether the value of revision is NULL. If revision is NULL, the operation of strcmp(revision, ext_plugins[u].revision) will lead to a crash.	2021-05-20	not yet calculated	CVE-2021-28904 CONFIRM
libyang -- libyang	In function lys_node_free() in libyang <= v1.0.225, it asserts that the value of node->module can't be NULL. But in some cases, node->module can be null, which triggers a reachable assertion (CWE-617).	2021-05-20	not yet calculated	CVE-2021-28905 CONFIRM
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Redirect module's redirection administration page in Liferay Portal 7.3.2 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_redirect_web_internal_portlet_RedirectPortlet_destinationURL parameter.	2021-05-17	not yet calculated	CVE-2021-29045 MISC MISC
liferay -- portal	The JSON web services in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 20 and 7.2 before fix pack 10 may provide overly verbose error messages, which allows remote attackers to use the contents of error messages to help launch another, more focused attacks via crafted inputs.	2021-05-16	not yet calculated	CVE-2021-29040 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
liferay -- portal	The SimpleCaptcha implementation in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.3 before fix pack 1 does not invalidate CAPTCHA answers after it is used, which allows remote attackers to repeatedly perform actions protected by a CAPTCHA challenge by reusing the same CAPTCHA answer.	2021-05-16	not yet calculated	CVE-2021-29047 MISC MISC
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Site module's membership request administration pages in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the <code>_com_liferay_site_my_sites_web_portlet_MySitesPortlet_comments</code> parameter.	2021-05-17	not yet calculated	CVE-2021-29044 MISC MISC
liferay -- portal	Denial-of-service (DoS) vulnerability in the Multi-Factor Authentication module in Liferay DXP 7.3 before fix pack 1 allows remote authenticated attackers to prevent any user from authenticating by (1) enabling Time-based One-time password (TOTP) on behalf of the other user or (2) modifying the other user's TOTP shared secret.	2021-05-16	not yet calculated	CVE-2021-29041 MISC MISC
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Layout module's page administration page in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.2 before fix pack 11 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the <code>_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_name</code> parameter.	2021-05-17	not yet calculated	CVE-2021-29048 MISC MISC
liferay -- portal	The Portal Store module in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 does not obfuscate the S3 store's proxy password, which allows attackers to steal the proxy password via man-in-the-middle attacks or shoulder surfing.	2021-05-17	not yet calculated	CVE-2021-29043 MISC MISC
liferay -- portal	Multiple SQL injection vulnerabilities in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1 allow remote authenticated users to execute arbitrary SQL commands via the classPKField parameter to (1) <code>CommerceChannelRelFinder.countByC_C</code> , or (2) <code>CommerceChannelRelFinder.findByC_C</code> .	2021-05-17	not yet calculated	CVE-2021-29053 MISC MISC
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Asset module's categories administration page in Liferay Portal 7.3.4 allows remote attackers to inject arbitrary web script or HTML via the site name.	2021-05-16	not yet calculated	CVE-2021-29039 MISC MISC
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Asset module's Asset Publisher app in Liferay Portal 7.2.1 through 7.3.5, and Liferay DXP 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the <code>_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_XXXXXXXXXX</code> parameter.	2021-05-17	not yet calculated	CVE-2021-29051 MISC MISC
liferay -- portal	The Data Engine module in Liferay Portal 7.3.0 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 does not check permissions in <code>DataDefinitionResourceImpl.getSiteDataDefinitionByContentTypeByDataDefinitionKey</code> which allows remote authenticated users to view DDMStructures via GET API calls.	2021-05-17	not yet calculated	CVE-2021-29052 MISC MISC
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Asset module's category selector input field in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1, allows remote attackers to inject arbitrary web script or HTML via the <code>_com_liferay_asset_categories_admin_web_portlet_AssetCategoriesAdminPortlet_title</code> parameter.	2021-05-17	not yet calculated	CVE-2021-29046 MISC MISC
linux -- linux_kernel	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of user-supplied eBPF programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-13661.	2021-05-21	not yet calculated	CVE-2021-31440 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	TCP firewalls could be circumvented by sending a SYN Packets with other flags (like e.g. RST flag) set, which was not correctly discarded by the Linux TCP stack after firewalling.	2021-05-18	not yet calculated	CVE-2002-2438 MLIST CERT-VN MLIST MISC MLIST MLIST MLIST MISC MLIST MLIST MISC MLIST MLIST MLIST
linux -- linux_kernel	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected	2021-05-17	not yet calculated	CVE-2021-3483 MLIST MISC
linux_kernel -- linux_kernel	The Linux kernel before 5.11.14 has a use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c because the CIPSO and CALIPSO refcounting for the DOI definitions is mishandled, aka CID-ad5d07f4a9cd. This leads to writing an arbitrary value.	2021-05-14	not yet calculated	CVE-2021-33033 MISC MISC MISC MISC MISC MISC
linux_kernel -- linux_kernel	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.	2021-05-14	not yet calculated	CVE-2021-33034 MISC MISC MISC MISC FEDORA
manageone -- manageone	There is a denial of service vulnerability in some versions of ManageOne. There is a logic error in the implementation of a function of a module. When the service pressure is heavy, there is a low probability that an exception may occur. Successful exploit may cause some services abnormal.	2021-05-20	not yet calculated	CVE-2021-22409 MISC
manageone -- manageone	There is a denial of service vulnerability in some versions of ManageOne. In specific scenarios, due to the insufficient verification of the parameter, an attacker may craft some specific parameter. Successful exploit may cause some services abnormal.	2021-05-20	not yet calculated	CVE-2021-22339 MISC
matrix-react-sdk -- matrix-react-sdk	Matrix-React-SDK is a react-based SDK for inserting a Matrix chat/voip client into a web page. Before version 3.21.0, when uploading a file, the local file preview can lead to execution of scripts embedded in the uploaded file. This can only occur after several user interactions to open the preview in a separate tab. This only impacts the local user while in the process of uploading. It cannot be exploited remotely or by other users. This vulnerability is patched in version 3.21.0.	2021-05-17	not yet calculated	CVE-2021-32622 MISC CONFIRM
micro-ecc -- library	The ECDSA operation of the micro-ecc library 1.0 is vulnerable to simple power analysis attacks which allows an adversary to extract the private ECC key.	2021-05-20	not yet calculated	CVE-2020-27209 MISC MISC MISC MISC
mikrotik -- routers	Mikrotik RouterOs before 6.47 (stable tree) in the /ram/pkg/advanced-tools/nova/bin/netwatch process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.	2021-05-19	not yet calculated	CVE-2020-20264 MISC MISC
mikrotik -- routers	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-18	not yet calculated	CVE-2020-20254 MISC FULLDISC
mikrotik -- routers	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/dot1x process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-05-19	not yet calculated	CVE-2020-20266 MISC MISC
mikrotik -- routers	Mikrotik RouterOs before 6.47 (stable tree) suffers from a division by zero vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.	2021-05-18	not yet calculated	CVE-2020-20253 MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mitsubishielectric -- multiple_products	Buffer access with incorrect length value vulnerability in GOT2000 series GT27 model communication driver versions 01.19.000 through 01.38.000, GT25 model communication driver versions 01.19.000 through 01.38.000, GT23 model communication driver versions 01.19.000 through 01.38.000 and GT21 model communication driver versions 01.21.000 through 01.39.000, GOT SIMPLE series GS21 model communication driver versions 01.21.000 through 01.39.000, GT SoftGOT2000 versions 1.170C through 1.250L and Tension Controller LE7-40GU-L Screen package data for MODBUS/TCP V1.00 allows a remote unauthenticated attacker to stop the communication function of the products via specially crafted packets.	2021-05-19	not yet calculated	CVE-2021-20589 MISC MISC
moodle -- mushtache	A vulnerability was found in Moodle where JavaScript injection was possible in some Mustache templates via recursive rendering from contexts. Mustache helper tags that were included in template contexts were not being escaped before that context was injected into another Mustache helper, which could result in script injection in some templates. This affects versions 3.7 to 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions.	2021-05-17	not yet calculated	CVE-2019-14827 MISC MISC
mozilla -- firefox	A flaw in Mozilla's embedded certificate code might allow web sites to install root certificates on devices without user approval.	2021-05-17	not yet calculated	CVE-2007-5967 MISC
mpv -- mpv	A format string vulnerability in mpv through 0.33.0 allows user-assisted remote attackers to achieve code execution via a crafted m3u playlist file.	2021-05-18	not yet calculated	CVE-2021-30145 MISC MISC MISC MISC
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';\$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3.	2021-05-21	not yet calculated	CVE-2021-33514 MISC MISC
nitrokey -- fido2	The flash read-out protection (RDP) level is not enforced during the device initialization phase of the SoloKeys Solo 4.0.0 & Somu and the Nitrokey FIDO2 token. This allows an adversary to downgrade the RDP level and access secrets such as private ECC keys from SRAM via the debug interface.	2021-05-21	not yet calculated	CVE-2020-27208 MISC MISC MISC MISC MISC
nitrokey -- fido_u2f	An issue was discovered in Nitrokey FIDO U2F firmware through 1.1. Communication between the microcontroller and the secure element transmits credentials in plain. This allows an adversary to eavesdrop the communication and derive the secrets stored in the microcontroller. As a result, the attacker is able to arbitrarily manipulate the firmware of the microcontroller.	2021-05-21	not yet calculated	CVE-2020-12061 MISC MISC MISC
nordic -- semiconductor_nrf52840_devices	Nordic Semiconductor nRF52840 devices through 2020-10-19 have improper protection against physical side channels. The flash read-out protection (APPROTECT) can be bypassed by injecting a fault during the boot phase.	2021-05-21	not yet calculated	CVE-2020-27211 MISC MISC MISC MISC
opc_foundation -- opc_foundation	Products with Unified Automation .NET based OPC UA Client/Server SDK Bundle: Versions V3.0.7 and prior (.NET 4.5, 4.0, and 3.5 Framework versions only) are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow.	2021-05-20	not yet calculated	CVE-2021-27434 MISC
opc_foundation -- opc_foundation	OPC Foundation UA .NET Standard versions prior to 1.4.365.48 and OPC UA .NET Legacy are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow.	2021-05-20	not yet calculated	CVE-2021-27432 MISC
openid -- providers	It was found that various OpenID Providers (OPs) had TLS Server Certificates that used weak keys, as a result of the Debian Predictable Random Number Generator (CVE-2008-0166). In combination with the DNS Cache Poisoning issue (CVE-2008-1447) and the fact that almost all SSL/TLS implementations do not consult CRLs (currently an untracked issue), this means that it is impossible to rely on these OPs.	2021-05-21	not yet calculated	CVE-2008-3280 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openldap -- openldap	A flaw was found in OpenLDAP. This flaw allows an attacker who can send a malicious packet to be processed by OpenLDAP's slapd server, to trigger an assertion failure. The highest threat from this vulnerability is to system availability.	2021-05-18	not yet calculated	CVE-2020-25709 MLIST DEBIAN MISC FULLDISC CONFIRM
opennms -- horizon	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `groupName` and `groupComment` parameters. Due to this flaw, an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files which can cause severe damage to the organization using opennms.	2021-05-20	not yet calculated	CVE-2021-25933 MISC MISC MISC MISC
opennms -- horizon	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection, and since there is no validation of an existing user name while renaming a user. As a result, privileges of the renamed user are being overwritten by the old user and the old user is being deleted from the user list.	2021-05-20	not yet calculated	CVE-2021-25930 MISC MISC MISC
opennms -- horizon	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection at `/opennms/admin/userGroupView/users/updateUser`. This flaw allows assigning `ROLE_ADMIN` security role to a normal user. Using this flaw, an attacker can trick the admin user to assign administrator privileges to a normal user by enticing him to click upon an attacker-controlled website.	2021-05-20	not yet calculated	CVE-2021-25931 MISC MISC MISC
opennms -- horizon	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting since there is no validation on the input being sent to the `name` parameter in `noticeWizard` endpoint. Due to this flaw an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files.	2021-05-20	not yet calculated	CVE-2021-25929 MISC MISC MISC
owncloud -- owncloud	ownCloud 10.7 has an incorrect access control vulnerability, leading to remote information disclosure. Due to a bug in the related API endpoint, the attacker can enumerate all users in a single request by entering three whitespaces. Secondary, the retrieval of all users on a large instance could cause higher than average load on the instance.	2021-05-20	not yet calculated	CVE-2021-29659 MISC MISC
pajbot -- pajbot	Pajbot is a Twitch chat bot. Pajbot versions prior to 1.52 are vulnerable to cross-site request forgery (CSRF). Hosters of the bot should upgrade to `v1.52` or `stable` to install the patch or, as a workaround, can add one modern dependency.	2021-05-20	not yet calculated	CVE-2021-32632 MISC MISC CONFIRM
phpmyadmin -- phpmyadmin	An information disclosure vulnerability was discovered in alipay_function.php in the log file of Alibaba payment interface on PHPPYUN prior to version 5.0.1. If exploited, this vulnerability will allow attackers to obtain users' personally identifiable information including e-mail address and telephone numbers.	2021-05-21	not yet calculated	CVE-2020-23768 MISC
plone -- plone	Plone through 5.2.4 allows XSS via a full name that is mishandled during rendering of the ownership tab of a content item.	2021-05-21	not yet calculated	CVE-2021-33508 MISC MLIST
plone -- plone	Plone through 5.2.4 allows stored XSS attacks (by a Contributor) by uploading an SVG or HTML document.	2021-05-21	not yet calculated	CVE-2021-33512 MISC MLIST
plone -- plone	Plone through 5.2.4 allows SSRF via the lxml parser. This affects Diazo themes, Dexterity TTW schemas, and modeeditors in plone.app.theming, plone.app.dexterity, and plone.supermodel.	2021-05-21	not yet calculated	CVE-2021-33511 MISC MLIST
plone -- plone	Plone through 5.2.4 allows remote authenticated managers to conduct SSRF attacks via an event ical URL, to read one line of a file.	2021-05-21	not yet calculated	CVE-2021-33510 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
plone -- plone	Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script.	2021-05-21	not yet calculated	CVE-2021-33509 MISC MLIST
plone -- plone	Plone through 5.2.4 allows XSS via the inline_diff methods in Products.CMFDiffTool.	2021-05-21	not yet calculated	CVE-2021-33513 MISC MLIST
plone_cms -- plone_cms	Plone CMS until version 5.2.4 has a stored Cross-Site Scripting (XSS) vulnerability in the user fullname property and the file upload functionality. The user's input data is not properly encoded when being echoed back to the user. This data can be interpreted as executable code by the browser and allows an attacker to execute JavaScript in the context of the victim's browser if the victim opens a vulnerable page containing an XSS payload.	2021-05-20	not yet calculated	CVE-2021-3313 MISC MISC MLIST
pluck -- pluck	In Pluck-4.7.10-dev2 admin background, a remote command execution vulnerability exists when uploading files.	2021-05-18	not yet calculated	CVE-2020-20951 MISC
pluck -- pluck	Cross Site Request Forgery (CSRF) in Pluck CMS v4.7.9 allows remote attackers to execute arbitrary code and delete specific images via the component " /admin.php?action=images."	2021-05-17	not yet calculated	CVE-2020-18198 MISC
pluck -- pluck	An issue was discovered in Pluck 4.7.10-dev2. There is a CSRF vulnerability that can editpage via a /admin.php?action=editpage	2021-05-18	not yet calculated	CVE-2020-24740 MISC
pluck -- pluck	Cross Site Request Forgery (CSRF) in Pluck CMS v4.7.9 allows remote attackers to execute arbitrary code and delete a specific article via the component " /admin.php?action=page."	2021-05-17	not yet calculated	CVE-2020-18195 MISC
postgresql -- postgresql	In the pg_partman (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit search_path is not set.	2021-05-19	not yet calculated	CVE-2021-33204 MISC MISC
progress -- moveit_transfer	In Progress MOVEit Transfer before 2021.0 (13.0), a SQL injection vulnerability has been found in the MOVEit Transfer web app that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements. This is in MOVEit.DMZ.WebApp in SILHuman.vb.	2021-05-18	not yet calculated	CVE-2021-31827 MISC MISC MISC
project_worlds -- online_examination_system	XSS in signup form in Project Worlds Online Examination System 1.0 allows remote attacker to inject arbitrary code via the name field	2021-05-17	not yet calculated	CVE-2020-29205 MISC MISC
prometheus -- prometheus	Prometheus is an open-source monitoring system and time series database. In 2.23.0, Prometheus changed its default UI to the New ui. To ensure a seamless transition, the URL's prefixed by /new redirect to /. Due to a bug in the code, it is possible for an attacker to craft an URL that can redirect to any other URL, in the /new endpoint. If a user visits a prometheus server with a specially crafted address, they can be redirected to an arbitrary URL. The issue was patched in the 2.26.1 and 2.27.1 releases. In 2.28.0, the /new endpoint will be removed completely. The workaround is to disable access to /new via a reverse proxy in front of Prometheus.	2021-05-19	not yet calculated	CVE-2021-29622 CONFIRM MISC MISC
putty -- putty	PutTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PutTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for similar reasons.	2021-05-21	not yet calculated	CVE-2021-33500 MISC MISC MISC
python -- python	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7.	2021-05-20	not yet calculated	CVE-2021-3426 FEDORA FEDORA FEDORA MLIST FEDORA FEDORA MISC FEDORA GENTOO FEDORA
qibosoftx1 -- qibosoftx1	A code injection vulnerability has been discovered in the Upgrade function of QibosoftX1 v1.0. An attacker is able execute arbitrary PHP code via exploitation of client_upgrade_edition.php and Upgrade.php.	2021-05-21	not yet calculated	CVE-2021-27811 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qnap -- nas	A relative path traversal vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to modify files that impact system integrity. QNAP have already fixed this vulnerability in the following versions: QTS 4.5.2.1630 Build 20210406 and later QTS 4.3.6.1663 Build 20210504 and later QTS 4.3.3.1624 Build 20210416 and later QuTS hero h4.5.2.1638 Build 20210414 and later QNAP NAS running QTS 4.5.3 are not affected.	2021-05-21	not yet calculated	CVE-2021-28798 CONFIRM
rabbitmq -- rabbitmq	RabbitMQ installers on Windows prior to version 3.8.16 do not harden plugin directory permissions, potentially allowing attackers with sufficient local filesystem permissions to add arbitrary plugins.	2021-05-18	not yet calculated	CVE-2021-22117 MISC
rageframe2 -- rageframe2	TinyShop, a free and open source mall based on RageFrame2, has a stored XSS vulnerability that affects version 1.2.0. TinyShop allows XSS via the explain_first and again_explain parameters of the /evaluate/index.php page. The vulnerability may be exploited remotely, resulting in cross-site scripting (XSS) or information disclosure.	2021-05-18	not yet calculated	CVE-2020-24026 MISC MISC MISC
red_hat -- red_hat	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created.	2021-05-17	not yet calculated	CVE-2021-3524 MISC FEDORA FEDORA FEDORA
red_hat -- red_hat	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a swift URL that ends with two slashes it can cause the rgw to crash, resulting in a denial of service. The greatest threat to the system is of availability.	2021-05-18	not yet calculated	CVE-2021-3531 MISC MLIST MLIST FEDORA FEDORA FEDORA
red_hat -- red_hat	A Zip Slip vulnerability was found in the oc binary in openshift-clients where an arbitrary file write is achieved by using a specially crafted raw container image (.tar file) which contains symbolic links. The vulnerability is limited to the command 'oc image extract'. If a symbolic link is first created pointing within the tarball, this allows further symbolic links to bypass the existing path check. This flaw allows the tarball to create links outside the tarball's parent directory, allowing for executables or configuration files to be overwritten, resulting in arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions up to and including openshift-clients-4.7.0-202104250659.p0.git.95881af are affected.	2021-05-14	not yet calculated	CVE-2020-27833 MISC CONFIRM
rfnftps -- firmware	RFNFTPS firmware versions System_01000004 and earlier, and Web_01000004 and earlier allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors.	2021-05-20	not yet calculated	CVE-2021-20719 MISC MISC
rxvt-unicode -- rxvt-unicode	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC G Q). A response is terminated by a newline.	2021-05-20	not yet calculated	CVE-2021-33477 MISC MISC MISC MISC MISC MISC MISC
searchblox -- searchblox	A local file inclusion vulnerability in the FileServlet in all SearchBlox before 9.2.2 allows remote, unauthenticated users to read arbitrary files from the operating system via a /searchblox/servlet/FileServlet?col=url= request. Additionally, this may be used to read the contents of the SearchBlox configuration file (e.g., searchblox/WEB-INF/config.xml), which contains both the Super Admin's API key and the base64 encoded SHA1 password hashes of other SearchBlox users.	2021-05-20	not yet calculated	CVE-2020-35580 MISC MISC
sitel -- cap/prx_firmware	SITEL CAP/PRX firmware version 5.2.01, allows an attacker with access to the device's network to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending HTTP requests massively.	2021-05-17	not yet calculated	CVE-2021-32455 CONFIRM
sitel -- cap/prx_firmware	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network of the device to obtain the authentication passwords by analysing the network traffic.	2021-05-17	not yet calculated	CVE-2021-32456 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sitel -- cap/prx_firmware	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network, to access via HTTP to the internal configuration database of the device without any authentication. An attacker could exploit this vulnerability in order to obtain information about the device's configuration.	2021-05-17	not yet calculated	CVE-2021-32453 CONFIRM
sitel -- cap/prx_firmware	SITEL CAP/PRX firmware version 5.2.01 makes use of a hardcoded password. An attacker with access to the device could modify these credentials, leaving the administrators of the device without access.	2021-05-17	not yet calculated	CVE-2021-32454 CONFIRM
slapi-nis -- slapi-nis	A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to crash the 389-ds-base directory server. The highest threat from this vulnerability is to system availability.	2021-05-20	not yet calculated	CVE-2021-3480 MISC
smartstore -- smartstore	An issue was discovered in Smartstore (aka SmartStoreNET) before 4.1.0. Administration/Controllers/ImportController.cs allows path traversal (for copy and delete actions) in the ImportController.Create method via a TempFileName field.	2021-05-19	not yet calculated	CVE-2020-36364 MISC MISC
smartstore -- smartstore	Smartstore (aka SmartStoreNET) before 4.1.0 allows CommonController.ClearCache, ClearDatabaseCache, RestartApplication, and ScheduleTaskController.Edit open redirect.	2021-05-19	not yet calculated	CVE-2020-36365 MISC
solarwinds -- network_performance_monitor	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12213.	2021-05-21	not yet calculated	CVE-2021-31474 MISC MISC
solarwinds -- orion_job_scheduler	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Job Scheduler 2020.2.1 HF 2. Authentication is required to exploit this vulnerability. The specific flaw exists within the JobRouterService WCF service. The issue is due to the WCF service configuration, which allows a critical resource to be accessed by unprivileged users. An attacker can leverage this vulnerability to execute code in the context of an administrator. Was ZDI-CAN-12007.	2021-05-21	not yet calculated	CVE-2021-31475 MISC MISC
sophos -- endpoint_products	In multiple versions of Sophos Endpoint products for MacOS, a local attacker could execute arbitrary code with administrator privileges.	2021-05-17	not yet calculated	CVE-2021-25264 CONFIRM MISC
stmicroelectronics -- stm32l4_devices	STMicroelectronics STM32L4 devices through 2020-10-19 have incorrect access control. The flash read-out protection (RDP) can be degraded from RDP level 2 (no access via debug interface) to level 1 (limited access via debug interface) by injecting a fault during the boot phase.	2021-05-21	not yet calculated	CVE-2020-27212 MISC MISC
stmicroelectronics -- stm32l4_devices	STMicroelectronics STM32L4 devices through 2021-03-29 have incorrect physical access control.	2021-05-21	not yet calculated	CVE-2021-29414 MISC
synology -- diskstation_manager	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology DiskStation Manager. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of DSI structures in Netatalk. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12326.	2021-05-21	not yet calculated	CVE-2021-31439 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Stack Based Overflow in the gray_split_cubic function of their custom fork of the rlttie library. A remote attacker might be able to overwrite Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31321 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LottieParserImpl::parseDashProperty function of their custom fork of the rlttie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31323 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion in the LOTComLayerItem::LOTComLayerItem function of their custom fork of the rllottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31318 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the VGradientCache::generateGradientColorTable function of their custom fork of the rllottie library. A remote attacker might be able to overwrite heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31320 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LOTGradient::populate function of their custom fork of the rllottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31322 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by an Integer Overflow in the LOTGradient::populate function of their custom fork of the rllottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31319 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion in the VDasher constructor of their custom fork of the rllottie library. A remote attacker might be able to access Telegram's heap memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31317 MISC MISC
telegram -- multiple_products	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Stack Based Overflow in the blit function of their custom fork of the rllottie library. A remote attacker might be able to access Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker.	2021-05-18	not yet calculated	CVE-2021-31315 MISC MISC
trusted_firmware-m -- trusted_firmware-m	In Trusted Firmware-M through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the event of a failure) can prevent the abort() operation in the associated cryptographic library from freeing internal resources, causing a memory leak.	2021-05-21	not yet calculated	CVE-2021-32032 CONFIRM MISC MISC
ubiquiti -- unifi_video	In Ubiquiti UniFi Video v3.10.13, when the executable starts, its first library validation is in the current directory. This allows the impersonation and modification of the library to execute code on the system. This was tested in (Windows 7 x64/Windows 10 x64).	2021-05-17	not yet calculated	CVE-2020-24755 MISC
vmd -- vmd	vmd through 1.34.0 allows 'div class="markdown-body"' XSS, as demonstrated by Electron remote code execution via require('child_process').execSync('calc.exe') on Windows and a similar attack on macOS.	2021-05-17	not yet calculated	CVE-2021-33041 MISC
websvn -- websvn	WebSVN before 2.6.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the search parameter.	2021-05-18	not yet calculated	CVE-2021-32305 MISC
wildfly -- wildfly	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity.	2021-05-20	not yet calculated	CVE-2021-3536 MISC
wordpress -- wordpress	The tab parameter of the settings page of the 404 SEO Redirection WordPress plugin through 1.3 is vulnerable to a reflected Cross-Site Scripting (XSS) issue as user input is not properly sanitised or escaped before being output in an attribute.	2021-05-17	not yet calculated	CVE-2021-24325 CONFIRM
wordpress -- wordpress	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled	2021-05-17	not yet calculated	CVE-2021-24323 CONFIRM
wordpress -- wordpress	The Happy Addons for Elementor WordPress plugin before 2.24.0, Happy Addons Pro for Elementor WordPress plugin before 1.17.0 have a number of widgets that are vulnerable to stored Cross-Site Scripting(XSS) by lower-privileged users such as contributors, all via a similar method: The "Card" widget accepts a "title_tag" parameter. Although the element control lists a fixed set of possible html tags, it is possible to send a 'save_builder' request with the "heading_tag" set to "script", and the actual "title" parameter set to JavaScript to be executed within the script tags added by the "heading_tag" parameter.	2021-05-17	not yet calculated	CVE-2021-24292 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The SEO Redirection Plugin "301 Redirect Manager" WordPress plugin before 6.4 did not sanitise the Redirect From and Redirect To fields when creating a new redirect in the dashboard, allowing high privilege users (even with the <code>unfiltered_html</code> disabled) to set XSS payloads	2021-05-17	not yet calculated	CVE-2021-24327 CONFIRM
wordpress -- wordpress	It was possible to exploit an Unauthenticated Time-Based Blind SQL Injection vulnerability in the Spam protection, AntiSpam, FireWall by CleanTalk WordPress Plugin before 5.153.4. The <code>update_log</code> function in <code>lib/Cleantalk/ApiWP/Firewall/SFW.php</code> included a vulnerable query that could be injected via the User-Agent Header by manipulating the cookies set by the Spam protection, AntiSpam, FireWall by CleanTalk WordPress plugin before 5.153.4, sending an initial request to obtain a <code>ct_sfw_pass_key</code> cookie and then manually setting a separate <code>ct_sfw_passed</code> cookie and disallowing it from being reset.	2021-05-17	not yet calculated	CVE-2021-24295 MISC CONFIRM
wordpress -- wordpress	There is functionality in the Store Locator Plus for WordPress plugin through 5.5.14 that made it possible for authenticated users to update their user meta data to become an administrator on any site using the plugin.	2021-05-17	not yet calculated	CVE-2021-24289 MISC CONFIRM
wordpress -- wordpress	The tab parameter of the settings page of the All 404 Redirect to Homepage WordPress plugin before 1.21 was vulnerable to an authenticated reflected Cross-Site Scripting (XSS) issue as user input was not properly sanitised before being output in an attribute.	2021-05-17	not yet calculated	CVE-2021-24326 CONFIRM
wordpress -- wordpress	There are several endpoints in the Store Locator Plus for WordPress plugin through 5.5.15 that could allow unauthenticated attackers the ability to inject malicious JavaScript into pages.	2021-05-17	not yet calculated	CVE-2021-24290 CONFIRM MISC
wordpress -- wordpress	The ReDi Restaurant Reservation WordPress plugin before 21.0426 provides the functionality to let users make restaurant reservations. These reservations are stored and can be listed on an 'Upcoming' page provided by the plugin. An unauthenticated user can fill in the form to make a restaurant reservation. The form to make a restaurant reservation field called 'Comment' does not use proper input validation and can be used to store XSS payloads. The XSS payloads will be executed when the plugin user goes to the 'Upcoming' page, which is an external website <code>https://upcoming.reservationdiary.eu/</code> loaded in an iframe, and the stored reservation with XSS payload is loaded.	2021-05-17	not yet calculated	CVE-2021-24299 CONFIRM
wordpress -- wordpress	The Goto WordPress theme before 2.1 did not sanitise, validate or escape the keywords GET parameter from its listing page before using it in a SQL statement, leading to an Unauthenticated SQL injection issue	2021-05-17	not yet calculated	CVE-2021-24314 CONFIRM MISC
wordpress -- wordpress	The GiveWP "Donation Plugin and Fundraising Platform" WordPress plugin before 2.10.4 did not sanitise or escape the Background Image field of its Stripe Checkout Setting and Logo field in its Email settings, leading to authenticated (admin+) Stored XSS issues.	2021-05-17	not yet calculated	CVE-2021-24315 MISC CONFIRM
wordpress -- wordpress	The 404 SEO Redirection WordPress plugin through 1.3 is lacking CSRF checks in all its settings, allowing attackers to make a logged in user change the plugin's settings. Due to the lack of sanitisation and escaping in some fields, it could also lead to Stored Cross-Site Scripting issues	2021-05-17	not yet calculated	CVE-2021-24324 CONFIRM
yara -- yara	An integer overflow and several buffer overflow reads in <code>libyara/modules/macho/macho.c</code> in YARA v4.0.3 and earlier could allow an attacker to either cause denial of service or information disclosure via a malicious Mach-O file. Affects all versions before libyara 4.0.4	2021-05-14	not yet calculated	CVE-2021-3402 MISC FEDORA FEDORA MISC MISC
zam64 -- zam64	Incorrect access control in <code>zam64.sys</code> , <code>zam32.sys</code> in MalwareFox AntiMalware 2.74.0.150 where <code>IOCTL's 0x80002014</code> , <code>0x80002018</code> expose unrestricted disk read/write capabilities respectively. A non-privileged process can open a handle to <code>\\.\ZemanaAntiMalware</code> , register with the driver using <code>IOCTL 0x80002010</code> and send these <code>IOCTL's</code> to escalate privileges by overwriting the boot sector or overwriting critical code in the pagefile.	2021-05-17	not yet calculated	CVE-2021-31727 MISC
zam64 -- zam64	Incorrect access control in <code>zam64.sys</code> , <code>zam32.sys</code> in MalwareFox AntiMalware 2.74.0.150 allows a non-privileged process to open a handle to <code>\\.\ZemanaAntiMalware</code> , register itself with the driver by sending <code>IOCTL 0x80002010</code> , allocate executable memory using a flaw in <code>IOCTL 0x80002040</code> , install a hook with <code>IOCTL 0x80002044</code> and execute the executable memory using this hook with <code>IOCTL 0x80002014</code> or <code>0x80002018</code> , this exposes ring 0 code execution in the context of the driver allowing the non-privileged process to elevate privileges.	2021-05-17	not yet calculated	CVE-2021-31728 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zmartzone -- mod_auth_openidc	mod_auth_openidc 2.4.0 to 2.4.7 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vectors.	2021-05-20	not yet calculated	CVE-2021-20718 MISC MISC MISC
zoho -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus before 6104 allows stored XSS on the /webclient/index.html#/directory-search user search page via the e-mail address field.	2021-05-20	not yet calculated	CVE-2021-27956 CONFIRM MISC MISC
zope -- zope	Zope Products.CMFCore before 2.5.1 and Products.PluggableAuthService before 2.6.2, as used in Plone through 5.2.4 and other products, allow Reflected XSS.	2021-05-21	not yet calculated	CVE-2021-33507 MISC MLIST
zope -- zope	Zope is an open-source web application server. In Zope versions prior to 4.6 and 5.2, users can access untrusted modules indirectly through Python modules that are available for direct use. By default, only users with the Manager role can add or edit Zope Page Templates through the web, but sites that allow untrusted users to add/edit Zope Page Templates through the web are at risk from this vulnerability. The problem has been fixed in Zope 5.2 and 4.6. As a workaround, a site administrator can restrict adding/editing Zope Page Templates through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page Templates through the web should be restricted to trusted users only.	2021-05-21	not yet calculated	CVE-2021-32633 MISC CONFIRM MLIST MLIST
zte -- axon_11_mobile_devices	A mobile phone of ZTE is impacted by improper access control vulnerability. Due to improper permission settings, third-party applications can read some files in the proc file system without authorization. Attackers could exploit this vulnerability to obtain sensitive information. This affects Axon 11 5G ZTE/CN_P725A12/P725A12:10/QKQ1.200816.002/20201116.175317:user/release-keys.	2021-05-19	not yet calculated	CVE-2021-21732 MISC
zxcdn -- zxcdn	The management system of ZXCDN is impacted by the information leak vulnerability. Attackers can make further analysis according to the information returned by the program, and then obtain some sensitive information. This affects ZXCDN V7.01 all versions up to IAMV7.01.01.02.	2021-05-19	not yet calculated	CVE-2021-21733 MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

Having trouble viewing this message? [View it as a webpage.](#)

You are subscribed to updates from the [Cybersecurity and Infrastructure Security Agency](#) (CISA)
[Manage Subscriptions](#) | [Privacy Policy](#) | [Help](#)

Connect with CISA:
[Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [YouTube](#)

Powered by



[Privacy Policy](#) | [Cookie Statement](#) | [Help](#)